carola frediani guerre di rete

i Robinson / Letture

Carola Frediani

Guerre di Rete

Editori Laterza

Sommario

Premessa

1. Hacker di Stato
   Ricercatori sotto attacco
   Apt: hacking di alto profilo
   Stuxnet: la prima arma digitale
   I cacciatori di Apt, tra ricerca e business
   Chi è l'attaccante?
   Infrastrutture critiche e cyber-guerre fredde
   Vi presento l'Apt più famoso: Apt28 o Sofacy
   Il labile confine tra azioni statali e criminali
   Il risiko statale degli Apt

2. Mercanti di attacchi
   AAA Vendesi vulnerabilità
   Bachi e codici di attacco
   Dai supermercati dell'hacking alle boutique per governi
   Trattative sotto banco
   Un mercato non regolato

3. Mi vendo il tuo database (e i tuoi tradimenti)
   Se il personale diventa pubblico
   Una marea di dati molto personali
   Sulle prime tracce
   L'arrivo dei piranha
   Alla ricerca di aiuto e risposte
   A caccia di Impact Team
   Un monito per tutti
   Dentro il commercio di dati

4. La fabbrica delle estorsioni
   Incontro col venditore
   L'esplosione dei ransomware, "i malware del ricatto"
   La filiera delle cyber-estorsioni

I programmi di affiliazione
Nascita e sviluppo di un modello di business cyber-criminale
Variazioni e innovazioni sul tema
Prevenire è meglio di curare
Geografia criminale

5. La cripto-guerra dei vent'anni
Nel cuore delle indagini informatiche
Lo scontro Fbi-Apple
Privacy contro sicurezza... o sicurezza contro sicurezza?
La prima cripto-guerra
Uno scontro mai sopito
Lo spettro delle backdoor
I dispositivi non sono fortezze

6. Reti di terrore
Paura e controllo
Le tre direttrici del dibattito Isis/Internet
Hacker pro-Isis

7. Frontiere della sorveglianza
Il progetto degli Emirati Arabi Uniti
L'attivista da un milione di dollari (e tre zero-day)
Altri esempi di sorveglianza e censura
I tanti modi per impossessarsi dei dati

8. Tor, o della complessità delle cipolle
Tutte le sfide di Tor
Storia di un progetto complesso
Mutamenti e controversie
Il Jakegate e la crisi interna di Tor

9. Vi presento: gli "attivisti della Rete"
A Valencia, nel nome della libertà digitale
La resistenza ai censori cinesi
Il ruolo delle aziende

Bibliografia

Glossario

Ringraziamenti

Come farò a raccontarvi, dunque?
Da insegnante, ho sempre insistito sulla semplicità.
Che si tratti di narrativa o di saggistica,
conta solo una domanda, e una risposta:
“Cosa accadde?”, chiede il lettore.
“Questo... e questo... e anche questo”,
risponde lo scrittore.
Farla semplice è il modo più sicuro.
Ci proverò, ma dovrete tenere presente che a Derry
la realtà è solo una sottile pellicola di ghiaccio
sulla superficie di un lago scuro e profondo.

Stephen King, 22/11/’63

Premessa

Questo è un libro sui conflitti di Rete, e in questa veste deve essere interpretato il titolo. Nessuna "cyberwar", quindi – termine abusato e retorico che richiama subito stellette e squilli di trombe –, bensì un tuffo in una serie di vicende molto concrete, a volte perfino sgangherate. Una serie di storie contemporanee, dunque, che attingono alla mia attività quotidiana di giornalista. È un lavoro improbo fissarle in un libro, poiché mentre chiudevo ogni capitolo la sua storia continuava a farsi e a disfarsi, ad aggiungere pezzi, a chiarire episodi, a confondere acque che si erano date per limpide e ferme. Se fare giornalismo su temi digitali è una corsa continua contro il tempo, scrivere un libro sugli stessi è una sorta di supplizio mitologico, una condanna che non ti permette mai di dire: ho finito. Ma se le storie restano aperte, i libri vanno chiusi: e sebbene il futuro prossimo sia già qui a rimescolare le carte, conto sul fatto che a restare saranno almeno alcuni messaggi: tra questi, la complessità tecnopolitica in cui siamo immersi.

Ho dunque provato a narrarla, questa complessità, in nove storie e capitoli indipendenti, e a loro modo concatenati; spezzoni di alcune tensioni socio-politiche che attraversano la Rete e che per mezzo di questa si esprimono. Dico alcune, perché in questo libro ci sono anche degli illustri assenti: come le grandi compagnie Internet e il loro ruolo all'interno del capitalismo dei dati (qualcuno lo chiama capitalismo della sorveglianza). Ma si tratta di un tema che merita un lavoro dedicato, mentre qui si è cercato di restringere il focus sulle espressioni più eclatanti ed esteriormente violente di questi conflitti.

Si parte con una panoramica al livello più alto, quello dell'"hacking" di Stato tra spionaggio e sabotaggio, della sotterranea guerra di posizionamento tra governi, loro agenzie e gruppi parastatali o schiettamente criminali, di cui di tanto in tanto fuoriescono eruzioni

improvvise e sorprendenti come quelle di un geyser. Un mondo sotterraneo alimentato da un crescente complesso cyber-industriale in cui attori, interessi e strumenti si mescolano e rimescolano in una lunga e opaca risacca.

E tuttavia, accanto ai ricercatori a caccia di software malevoli, accanto ai gruppi di hacker che colpiscono industrie in modo sofisticato, accanto ai venditori e ai broker di attacchi informatici, ci sono anche gli utenti comuni, carne da cannone di un crescente scenario di (in)sicurezza informatica dove ai primi virus artigianali si sono sostituite articolate filiere cyber-criminali in continua ricerca di modelli di business – e di vittime da spolpare. Sullo sfondo il riaccendersi delle tensioni, mai del tutto spente, sulla crittografia, ravvivate dalla paura del terrorismo e dalle false dicotomie che contrappongono privacy e sicurezza. O le frontiere selvagge, dinamiche, nebbiose della sorveglianza statale. Infine, a chiudere con un filo di speranza, l'attivismo di chi – pur essendo immerso fino al collo in questi conflitti nonché nelle proprie contraddizioni – ancora lavora per l'idea di una Rete al servizio delle persone e dei loro diritti.

1.
Hacker di Stato

Ricercatori sotto attacco

Quando Costin Raiu e sua moglie rientrarono a casa loro a Bucarest, intorno alle sette di sera del 29 novembre 2010, trovarono qualcosa di inaspettato. Un cubo posato sul tavolo del salotto. Lo stesso tavolo su cui avevano fatto colazione quella mattina e che avevano pulito prima di uscire. Il cubo era uno di quei dadi delle decisioni, che hanno una risposta diversa su ogni faccia – "Sì", "No", "Forse", ecc. – e che possono essere interrogati giocosamente come una Pizia formato Ikea. Quello che qualcuno, entrando in casa di Raiu, aveva lasciato sul tavolo, sulla faccia superiore esponeva la scritta: "Prenditi una pausa". Più che giocoso, suonava alquanto sinistro.

La vacanza che Raiu avrebbe dovuto prendersi era dall'ultima investigazione cui si stava dedicando. Non che lui lavori nell'intelligence, e tanto meno faccia l'investigatore privato. Semplicemente, fa analisi di software malevoli (detti anche "malware", da "malicious software"). È uno che passa il tempo a studiare il comportamento di un virus sconosciuto in un laboratorio virtuale, per ricostruirne le funzioni, la struttura, il codice, le tracce che ha lasciato per la Rete, e nel migliore dei casi i suoi autori.

Raiu – all'epoca trentatreenne – ha un'aria pacata, una voce calma e tranquilla, un viso affabile dietro gli occhiali da geek. Ama giocare a scacchi, la chimica, la fotografia. Difficile immaginarlo in una situazione alla James Bond come quella appena descritta. Dal padre ingegnere ha ereditato e sviluppato, fin da bambino, la passione per l'elettronica. Nel 1990, poco dopo la rivoluzione rumena, mentre il Paese si sta aprendo ai prodotti stranieri, mette le mani sul suo primo pc e inizia a programmare. Quando la sua scuola viene colpita e messa KO da un virus, lui passa la

notte a scrivere da zero uno strumento per individuarlo e pulire i pc. Raiu viene assunto da una azienda informatica rumena, la Gcad, e il suo strumento diventa un antivirus di nome Rav (Romanian Anti-Virus), successivamente acquistato da Microsoft. Nel frattempo, però, Raiu è passato a lavorare con il russo Eugene Kaspersky e la sua omonima società di cyber-sicurezza. Nel 2010 sono dieci anni che fa il ricercatore, da Bucarest, per quello che è ormai diventato un colosso del settore, ed è appena stato nominato direttore della squadra dedicata a indagare sui virus più ostici.

Il 2010 è un anno interessante per chi si occupa di malware. A gennaio gli ispettori dell'Agenzia internazionale per l'energia atomica (Aiea), incaricati di visitare l'impianto di arricchimento dell'uranio di Natanz, in Iran, notano dei malfunzionamenti nelle sue centrifughe, che devono essere sostituite più frequentemente della media. Nessuno all'epoca, nemmeno i tecnici iraniani, sembra conoscerne la ragione. Ma pochi mesi dopo Sergey Ulasen, un esperto di sicurezza informatica bielorusso che lavora per la VirusBlokAda, una piccola azienda di Minsk, viene contattato da alcuni suoi clienti in Iran, in panico per una sorta di epidemia che ha colpito i loro pc, che si bloccano mostrando delle schermate blu di errore (dette anche le schermate blu della morte di Windows) e altri malfunzionamenti. Con i suoi colleghi si mette al lavoro e in breve tempo comprende di avere davanti un malware sofisticato e potente, anche se del tutto misterioso in quel momento. Non si capisce chi voglia colpire, cosa debba fare e tanto meno chi lo abbia realizzato. Ulasen e colleghi pubblicano un post che attira l'attenzione di molti addetti ai lavori. Qualcuno inizia a connettere Stuxnet – così viene chiamato il malware misterioso, per la precisione un "worm", cioè un tipo di software malevolo che può replicarsi e diffondersi attraverso una rete – ad alcuni sistemi di controllo industriale della Siemens. Altri inizieranno a ipotizzare che possa esserci una relazione con il programma nucleare iraniano. Il ricercatore tedesco Ralph Langner si rende conto che il software malevolo esamina il sistema su cui si trova e, solo nel caso presenti specifiche caratteristiche, spegne alcuni processi. Insomma, è progettato per arrivare a dei target ben precisi.

Di lì a poco tutta una serie di esperti di diverse società e Paesi iniziano a cercare di capire qualcosa di più di questo malware. Tra questi ci sono anche Costin Raiu e i suoi colleghi a Kaspersky. "Il worm Stuxnet: un

cyber-missile contro l'Iran?", si chiede l'"Economist" nel settembre 2010. Pochi giorni dopo, Raiu vola a Vancouver per partecipare a una conferenza di cyber-sicurezza. Il suo è uno dei paper presentati all'ultimo momento, proprio per l'attualità dei temi trattati, e riguarda Stuxnet. "In realtà sostituivo il mio collega Alex Gostev che non aveva ottenuto il visto e mi aveva chiesto di andare al suo posto. All'epoca non ero neanche particolarmente coinvolto nello studio di questo malware", mi racconta Raiu al telefono. Durante la sua presentazione, però, si accorge di qualcosa di strano. "Mentre parlavo notai tre persone che stavano in piedi all'ultima fila e non sembravano molto contente. Erano venute solo per il mio intervento, per entrare avevano pagato in contanti alcune migliaia di dollari e se ne andarono senza fare domande".

Due mesi dopo, Raiu ha trovato quel cubo sul tavolo. "Mi ha colpito anche il fatto che il dado stava nel nostro ufficio, e da lì era stato spostato a casa mia, a suggerire che chi lo aveva lasciato lì poteva accedere a entrambi i luoghi", continua Raiu. "Naturalmente è stato qualcosa che mi ha colto di sorpresa e mi ha spaventato, anche perché ti chiedi se oltre al dado non sia stato aggiunto qualcos'altro in casa tua, strumenti di sorveglianza e via dicendo". Da allora Raiu ha rafforzato le sue misure personali di sicurezza, a partire dalle comunicazioni, tutte cifrate. "Nel mondo di chi lavora sull'analisi di questo genere di attacchi di natura statale si trova sempre qualcuno che ha storie simili, anche se molti preferiscono non parlarne".

Chi ha provato a raccogliere le loro storie è stata Andrada Fiscutean, una giornalista rumena che, oltre a lavorare per la radio Pro Fm di Bucarest, scrive per varie testate americane. "Mi sono interessata all'argomento dopo aver saputo di un ricercatore di cyber-sicurezza che aveva ricevuto minacce", mi racconta Fiscutean, che ho incontrato a un evento internazionale. "Era qualcosa di stupefacente, eppure nessuno ne aveva scritto. Mi è stato detto che questo genere di incidenti sono piuttosto comuni nel settore. La mia fonte era solida, eppure restavo scettica, non avevo mai sentito storie del genere pur seguendo temi tecnologici e affini da anni". Allora Fiscutean, che è una giovane donna dall'aria tanto tranquilla quanto determinata, ha iniziato a interrogare una serie di esperti che analizzavano malware per lavoro, riuscendo a parlare con una ventina di persone. "Tutti mi hanno confermato che questo tipo di situazioni accadono nella loro comunità".

Dopo aver pubblicato il suo articolo sulla rivista “Motherboard”, un’altra dozzina di addetti ai lavori l’hanno cercata per dirle che sapevano di analoghi incidenti capitati a loro o ad altri. Tuttavia la maggioranza ha preferito non rilasciare dichiarazioni pubbliche. Non si tratta di semplice paranoia, anche se molti hanno ammesso che vivere queste esperienze determina un mutamento di percezione e abitudini, un innalzamento delle difese e dell’attenzione. “Uno dei ricercatori che ho contattato, e il cui pc è stato hackerato da una entità statale, presumibilmente l’Agenzia di sicurezza nazionale americana (Nsa) o la sua equivalente britannica Gchq, mi ha fatto un test. Siccome è stato hackerato attraverso una richiesta di contatto su LinkedIn inviata da un profilo finto, cliccando sulla quale ha scaricato uno ‘spyware’ nel proprio pc, mi ha inviato una richiesta di amicizia proprio attraverso LinkedIn. Non ho cliccato sul pulsante *Accetta*, come aveva fatto lui, ma gli ho scritto via mail chiedendo se davvero era lui ad avermi contattato. Lui mi ha risposto: ‘Brava, hai capito a cosa bisogna stare attenti’”.

Altri le hanno spiegato che non usano mai l’infrastruttura cellulare Gsm per parlare: insomma, non usano le normali comunicazioni telefoniche. E lo stesso mi hanno detto alcuni ricercatori con cui ho avuto a che fare: solo telefonate cifrate attraverso app come Signal. “Alcuni usano un laptop diverso quando viaggiano”, prosegue Fiscutean. “Tuttavia, se devono lasciare il pc in hotel, lo chiudono e ci posizionano sopra alcuni cavi che poi fotografano. Se qualcuno entra e apre il laptop, non sarà in grado di riposizionarli nella stessa identica configurazione”.

Quando ho partecipato a un evento organizzato dalla società di cyber-sicurezza F-Secure, a Helsinki, tutti gli invitati hanno ricevuto in hotel un piccolo gadget: dello smalto per unghie con glitter. Se lasciate il computer in stanza – diceva il foglietto che lo accompagnava – sigillatelo con un adesivo su cui avete passato lo smalto e scattate una foto. Nel caso qualcuno provasse ad aprirlo, è quasi impossibile replicare i disegni dei grumi di brillantini nello stesso modo.

Sebbene i computer usati dai ricercatori siano protetti con una cifratura completa del disco, per cui senza conoscere la password è impossibile accedere ai loro contenuti, potrebbero infatti essere ancora vulnerabili a quello che si chiama “attacco della cameriera malvagia” (“evil maid attack”). Se un attaccante ha accesso fisico al pc (nello scenario in

questione, mentre si trova nella stanza d'albergo), potrebbe comunque avviarlo usando una unità disco separata e caricare sul sistema un "boot loader" modificato. Il boot loader è un programma che carica il "kernel" di un sistema operativo (ovvero il suo fulcro, nucleo, la parte che comunica con l'hardware) e ne permette l'avvio. Quando il proprietario del pc ritorna e avvia di nuovo il suo computer, si carica il boot loader maligno, e a quel punto si potrà catturare la sua password quando viene immessa per poi inviarla all'attaccante appena la macchina si connette a Internet.

"Non è raro sentire storie di informatici che, dopo aver diffuso la notizia di essere in possesso di certi 'exploit' rari e pregiati, ovvero di attacchi che sfruttano la vulnerabilità di alcuni software, venduti anche a caro prezzo nel mercato informatico, si siano accorti di aver ricevuto visite nelle loro stanze d'albergo. Probabilmente chi è entrato ha provato a vedere se si poteva sfruttare un evil maid attack, dove appunto rimpiazzi il boot loader e poi catturi i dati (in gergo, li 'esfiltri') quando l'utente riutilizza il pc", mi spiega Andrea Barisani, ricercatore triestino d'origine e di statura internazionale, che lavora proprio sulla realizzazione di sistemi software e hardware altamente sicuri.

Insomma, per dirla con le parole di Bruce Schneier, noto esperto di crittografia: "Non appena qualcuno ha accesso fisico al tuo computer, è andata". Ovviamente, dando per scontato che l'attaccante sia di caratura statale. E questo spiega perché, in certi ambienti a metà fra sicurezza informatica e attivismo, le persone girino sempre con zaino in spalla e computer appresso.

Fiscutean mi dice che molti ricercatori le hanno elencato varie strategie con cui difendono o nascondono le proprie comunicazioni e i propri apparecchi. "Alcuni, quando intrattengono di persona conversazioni private delicate, usano 'gabbie di Faraday'". Si tratta di contenitori fatti di materiali conduttori che isolano l'interno da campi elettromagnetici esterni. Questo fa sì che in nessun modo gli apparecchi, così schermati e isolati da segnali, possano essere usati da un attaccante per registrare conversazioni fra presenti.

L'uso di gabbie o sacche di Faraday dove mettere smartphone e pc in certe situazioni è una pratica che mi è stata confermata anche da alcuni attivisti e accademici che lavorano sul tema privacy/sorveglianza, e che per ovvie ragioni preferiscono non essere menzionati in questo caso. "Sul

portatile ho un sistema operativo di nome Qubes, che fra le altre cose implementa una funzione apposita contro l'evil maid attack", mi spiega uno di loro. "Inoltre ho un portafoglio particolare che scherma i chip di nuova generazione delle carte di credito – che permettono pagamenti senza contatto, avvicinando solo la carta ai lettori degli esercenti – per impedire che i loro dati possano essere letti da un attaccante che mi passi vicino. In generale, comunque, non lascio mai i miei apparecchi incustoditi. Tengo le mie identità digitali separate, anche su macchine diverse. Uso tenere il Wi-Fi del cellulare spento quando vado in giro. E ovviamente non navigo e se possibile non comunico in chiaro (ma solo attraverso sistemi di cifratura) da tre anni".

Apt: hacking di alto profilo

Come vedremo, Stuxnet è stato un attacco sponsorizzato da uno Stato. Ma cosa si intende con questa espressione? Negli ultimi anni si è diffusa una definizione apposita, Apt, che sta per "Advanced persistent threat", "minaccia persistente avanzata". Indica un tipo di incursione informatica di livello più alto di quelli della criminalità comune, che punta a obiettivi specifici, che è silenziosa e prolungata nel tempo, e che tendenzialmente cerca di esfiltrare dati o in casi più rari sabotare sistemi. In genere ha alle spalle una certa quantità di risorse e organizzazione. Insomma, Apt è la sigla tecnica e asettica per indicare l'innominabile: gruppi statali o parastatali che penetrano in modo ostile nelle reti di un'altra nazione o di una grande impresa o di singoli pc di particolare interesse. Ma anche gruppi criminali in grado di sferrare aggressioni di questo tipo, sia pure basate su altre motivazioni.

I primi a elaborare un rapporto dettagliato che svelava l'esistenza e l'identikit di un gruppo simile sono stati gli analisti di Mandiant – società oggi parte della compagnia statunitense FireEye, con forti legami con il governo Usa – quando nel 2013 pubblicarono il report intitolato *Apt1*[1]. Nel documento esponevano attività, infrastruttura e origine di un gruppo di cyber-spionaggio cinese riconducibile, anche fisicamente, all'unità 61398 dell'esercito della Repubblica popolare, unità in parte collocata in un palazzo di dodici piani a Shanghai. Oggi alla Cina sono attribuiti almeno nove gruppi di questo tipo, con nomi come Blue Termite,

Elederwood o Deep Panda. Quest'ultimo è stato tracciato a ritroso, da società di cyber-sicurezza americane, almeno fino al 2011. Considerato tra le entità di spionaggio digitale più sofisticate, gli sono attribuite molte intrusioni informatiche nelle reti governative statunitensi, per rubare segreti industriali e militari. Ad esempio, l'"OPM hack", ovvero l'attacco che nel 2015 ha sottratto i dati personali di 21 milioni di impiegati federali americani – e delle impronte digitali di 5,6 milioni –, è stato attribuito a Deep Panda. Secondo gli analisti occidentali, gli hacker cinesi starebbero ammassando enormi archivi di dati e di intelligence sui rivali a stelle e strisce.

Stuxnet: la prima arma digitale

Il fenomeno dell'hacking statale o parastatale esisteva già da tempo, ovviamente, anche se più contenuto e sotto traccia. In un certo senso, l'anno zero – in cui si è strappato il cielo di carta – è stato il 2010, con la scoperta di Stuxnet. Questo malware – come abbiamo visto – ha alterato di nascosto la velocità delle centrifughe dell'impianto per l'arricchimento dell'uranio a Natanz, in Iran, portando alla sostituzione forzata di mille macchine.

E questa è la prima novità: diversamente da altri virus o worm che puntavano a rubare informazioni o a violare e danneggiare sistemi informatici, Stuxnet realizzava, attraverso i computer, un'operazione di sabotaggio fisico. Il software malevolo era concepito in modo tale da modificare anche le informazioni che arrivavano ai tecnici, così che non si accorgessero della natura del malfunzionamento e la attribuissero ad altre cause.

Secondo il già citato Ralph Langner, il 50 per cento dei costi di sviluppo di Stuxnet è probabilmente andato nel tentativo di nasconderlo. Il malware era estremamente sofisticato. Usava ben quattro "zero-day", ovvero vulnerabilità di un software che non sono ancora note a nessuno se non all'attaccante. Si chiamano così perché gli sviluppatori dei programmi vulnerabili, non avendo idea della loro esistenza, hanno avuto "zero" giorni a disposizione per metterle a posto. Inoltre Stuxnet ha dovuto anche aggirare il fatto che i computer di controllo del sistema da attaccare non fossero collegati a Internet. Per saltare questo "vuoto d'aria", il fatto cioè

che i pc fossero separati dalla Rete, ha utilizzato come vettore d'attacco delle chiavette Usb. Gli attaccanti hanno prima infettato i computer di almeno quattro aziende esterne all'impianto di Natanz, che però erano connesse al programma nucleare iraniano o erano suoi fornitori, e da lì sono arrivati al loro target finale.

Ci sono state varie versioni di Stuxnet, in un crescendo di aggressività del malware. Tecnicamente era un worm, un virus che si sparge – oltre che per mezzo di Usb drive – attraverso la Rete. Pur potendo replicarsi e diffondersi su molti computer, rimaneva dormiente provocando solo misteriosi malfunzionamenti se non incontrava particolari condizioni, se non si trovava cioè su una macchina di un sistema di controllo industriale con specifiche configurazioni. Di fatto, però, Stuxnet col tempo si è diffuso in un centinaio di Paesi: qualcuno ha contato 300mila infezioni[2].

Altra novità di questo malware è che nasce apertamente da un progetto statale. Nel 2012 è arrivata la conferma di quello che molti sospettavano: e cioè che Stuxnet è il frutto di una collaborazione statunitense-israeliana. In particolare faceva parte del piano americano "Olympic Games" – avviato sotto la presidenza di George W. Bush – che voleva sabotare il programma nucleare iraniano con un attacco informatico. Stuxnet è stata dunque la prima arma digitale sviluppata da uno Stato ed effettivamente usata a scopi offensivi. Secondo alcuni osservatori, l'impiego di questo malware avrebbe avuto il merito di impedire un intervento militare vero e proprio. Una "bomba digitale" avrebbe ottenuto effetti simili a quelli di un'incursione fisica ma in modo discreto e sotterraneo, danneggiando le centrifughe silenziosamente per mesi senza dare nell'occhio. Uno dei suoi vantaggi fondamentali era la possibilità di intervenire di nascosto e, qualora il malware fosse stato scoperto, di negare in modo plausibile di esserne i mandanti. C'è un'espressione tecnica, usata sia nello spionaggio sia nella sicurezza informatica, per indicare questa mossa: *plausible deniability*, appunto negazione (letteralmente, negabilità) plausibile.

Tuttavia, a medio e lungo termine, Stuxnet ha avuto anche alcune importanti ripercussioni negative. Proprio mentre gli Stati Uniti condannavano le incursioni di cyber-spionaggio cinese, aver rilasciato la prima arma digitale conosciuta li ha messi nella posizione di non poter più predicare astinenza agli altri, come ha notato Kim Zetter nel suo libro *Countdown to Zero Day*[3]. "Il rilascio del malware ha lanciato una corsa alle

armi digitali tra Paesi piccoli e grandi che altererà per sempre lo scenario dei cyber-attacchi", ha scritto la giornalista di "Wired".

Peraltro – sostiene il documentario *Zero Days*[4] di Alex Gibney, uscito nel 2016 – Stuxnet sarebbe stato solo un tassello di una campagna di hacking molto più vasta e articolata, nome in codice "Nitro Zeus", che aveva penetrato surrettiziamente una serie di infrastrutture critiche iraniane, cioè di quei sistemi vitali per il funzionamento di uno Stato, dall'energia ai trasporti alla difesa. E che avrebbe potuto innescare ulteriori scenari di cyber-guerra.

Ricordiamo che negli anni di maggior tensione sul programma nucleare di Teheran – tra il 2008 e il 2011 – si è svolta una guerra non detta fra le potenze in gioco, che non si è limitata all'hacking. Diversi scienziati e accademici iraniani collegati al programma sono stati assassinati in modo clamoroso. Il 29 novembre 2010, nello stesso periodo in cui Stuxnet veniva progressivamente svelato al mondo e il giorno esatto in cui Costin Raiu trovava il cubo con il suggerimento di prendersi un po' di relax, Majid Shahriari, professore quarantenne di fisica nucleare con un ruolo rilevante nei progetti atomici di Teheran, veniva ucciso dentro la sua auto in mezzo al traffico e in pieno giorno. Alcuni motociclisti si sono avvicinati alla sua Peugeot Sedan e hanno attaccato una bomba alla portiera. Il tempo di sgommare via, poi l'esplosione, che ha ucciso lo scienziato e ferito gli altri due passeggeri, la moglie e la guardia del corpo. Poco tempo dopo, analoga sorte è toccata a un altro esperto iraniano di nucleare, il cinquantaduenne Fereydoon Abbasi, che però è riuscito a uscire dall'auto in tempo e si è salvato, trascinando fuori la moglie. Ancora all'inizio del 2012, la stessa modalità di attacco ha ucciso Mostafa Ahmadi Roshan, trentaduenne vicedirettore per le relazioni commerciali all'impianto di Natanz. E la lista potrebbe continuare.

Ad ogni modo, uno degli effetti collaterali di Stuxnet – e della sua scoperta – è stato di convincere l'Iran a investire nel campo cyber. Negli ultimi anni Teheran ha messo in piedi un piccolo esercito di hacker finanziato con circa 20 milioni di dollari, il quarto al mondo per numero di unità dopo Russia, Cina e Stati Uniti. Un esercito che è stato più spesso all'offensiva che in difesa, lanciando una serie di attacchi al settore finanziario americano. Aggressioni che, almeno secondo il Dipartimento di Giustizia statunitense, sarebbero costate decine di milioni di dollari alle

banche Usa. A queste è seguita una pesantissima incursione nella rete della compagnia petrolifera statale saudita Saudi Aramco, che ha messo KO 35mila computer, obbligando i suoi impiegati a ricorrere a carta e penna per svolgere molte delle loro attività. Gli hacker iraniani si sarebbero infiltrati nei sistemi attraverso una banale mail di "phishing" inviata a un dipendente, cioè una mail che arriva da un finto mittente e che contiene un malware.

I cacciatori di Apt, tra ricerca e business

Negli ultimi anni gli Apt, i gruppi di attacchi persistenti e avanzati dietro cui stanno organizzazioni strutturate – statali, parastatali o criminali –, sembrano essere proliferati. In parte, questa proliferazione è dovuta al crescente sforzo da parte di aziende di sicurezza di individuare e descrivere apertamente il fenomeno. Si sono, cioè, moltiplicati i rapporti rilasciati su queste entità da parte di compagnie private. Ovviamente molte di queste aziende competono fra loro sul mercato anche in termini di eccellenza e autorevolezza, per cui mostrare di essere capaci di individuare una minaccia informatica, qualunque essa sia, e tanto più se è sofisticata, è un asset fondamentale, anche soltanto come marketing. E tuttavia va detto che tali aziende, anche quando sono multinazionali, hanno comunque un'origine o un legame con un determinato Stato. Il che significa che in alcuni frangenti preferiscono concentrarsi sugli Apt collegati a determinati governi, rispetto a quelli foraggiati dal proprio. O che, a seconda dei casi, possono essere più o meno inclini a esplicitare l'origine di un attacco e a dichiararne il "mandante". Tutto ciò crea un quadro complesso, di cui si deve tenere conto quando si ha a che fare con tali report.

Tra i colossi del settore ci sono le già citate FireEye, americana, che ha lavorato molto sulle cyber-spie cinesi, e la russa Kaspersky, che ha individuato gruppi come Equation (attribuito agli Usa), o studiato malware quali Stuxnet e i suoi successori. In verità Kaspersky ha fatto della caccia agli Apt – statali e non – uno dei suoi elementi distintivi. Lo si capisce dal tenore delle sessioni e degli invitati alle sue conferenze annuali, oltre che dalle felpe nere con cappuccio distribuite per l'occasione, su cui spiccano i nomi di malware o Apt famosi, come appunto Stuxnet.

Il summit del 2016 ha portato sull'isola di Tenerife decine di ricercatori,

non solo dipendenti della società russa ma anche di imprese concorrenti come iSight o Check Point, e più in generale il Gotha della cyber-sicurezza mondiale. Poliziotti e loro consulenti come l'olandese Peter Kruse; sviluppatori di software Osint (cioè di intelligence su fonti aperte) come quelli che hanno creato il software Maltego; aziende che lavorano sull'antiterrorismo e l'analisi dei "big data" come Recorded Future; rappresentanti di Microsoft e Google; agenti dell'Fbi e via dicendo.

I tre giorni di conferenze – chiusi con un party pirotecnico tra disco, ballerini, parrucche, luci stroboscopiche, fiumi di alcol, insomma non esattamente il genere di cene "corporate" cui normalmente si è abituati – avevano come *leitmotiv* la caccia a gruppi, vecchi o nuovi, di Apt. Che si trattasse di criminali russi specializzati in articolate frodi bancarie o di misteriose entità latino-americane che mescolano spionaggio con estorsioni o, ancora, di emergenti malware mediorientali, è risultato evidente che l'ambizione di alcune delle aziende nel settore non è più quella di realizzare solo degli antivirus, bensì di proporsi come soggetti di cyber-intelligence. Come già detto, c'è *anche* una strategia di marketing. Ma è pur vero che le minacce informatiche negli ultimi anni si sono evolute, e lo scenario si è fatto più complicato.

Gli stessi esperti del settore ne sono sempre più consapevoli. Uno dei panel conclusivi della "due giorni" a Tenerife s'intitolava: *Lezioni dal mondo reale sulle spie che ogni ricercatore dovrebbe sapere*. In una delle sale dell'hotel Ritz-Carlton, dove si sono susseguiti workshop anche molto tecnici sui malware – finiti immancabilmente con uno shot di whisky per i relatori sul palco – due veterani di Kaspersky, Stefan Tanase e David Jacoby, hanno intrattenuto una platea sempre più rilassata e divertita (e composta al 90 per cento da giovani uomini in jeans e maglietta) sui pericoli dell'era analogica. Qui sono stati elencati aneddoti di ricercatori abbordati in modo aggressivo da qualche *femme fatale* al rientro in hotel, o ritrovatisi in aereo con un vicino di posto particolarmente curioso e bene informato su quello che facevano. Insomma, per un momento le lancette dell'orologio – dopo ore di sedute su *botnet*[5], spyware e vulnerabilità delle app – sembravano essere tornate indietro ai tempi del film *GoldenEye*. Con l'esiguità della rappresentanza femminile tra gli "analisti" presenti a rendere la situazione ancora più surreale.

Ma questi racconti, per quanto apparentemente folcloristici – come pure

quelli più inquietanti raccontati all'inizio del libro –, sono la spia di una transizione importante nel mondo della sicurezza informatica. Perché è vero che alcuni ricercatori, talvolta, possono trovarsi a maneggiare informazioni riservate di grande valore economico. O geopolitico. O addirittura militare. "L'industria della sicurezza informatica al suo più alto livello ha subìto un cambiamento epocale", ha scritto in un saggio Juan Andrés Guerrero-Saade[6], analista di Kaspersky. "I ricercatori si trovano sempre più spesso a investigare notevoli minacce geopolitiche o sponsorizzate da Stati. Come conseguenza, l'esperto di cyber-sicurezza, un tempo persona affabile e attenta alla comunità, è diventato un broker di intelligence, spesso frainteso e minacciato. In molti casi, i ricercatori non hanno voluto accettare questa realtà, né sono preparati ad affrontare questo loro nuovo ruolo".

Non solo: né loro, né le società per cui lavorano hanno le protezioni legali o politiche di cui normalmente godono gli apparati di intelligence veri e propri, prosegue Guerrero-Saade. Il problema, però, non è solo di natura personale, non riguarda solo chi lavora in questo settore, ma anche il risultato di tale lavoro. L'analista di Kaspersky spiega infatti una questione fondamentale e di cui si parla poco: l'effettiva qualità e attendibilità dei rapporti di cyber-intelligence, ormai prodotti da una miriade di aziende e destinati a diventare sempre più importanti, con conseguenze rilevanti. In prospettiva, un'analisi che punti il dito contro uno Stato, indicandolo come il mandante di una pesante aggressione digitale, potrebbe innescare veri e propri conflitti.

La posta in gioco, insomma, si sta alzando, e forse non sta facendo altrettanto la capacità di analisi. L'espressione Apt – riconosce Guerrero-Saade – è un termine ombrello che si applica a casi molto diversi a spese dell'accuratezza dell'analisi e della comprensione del fenomeno. Troppo facilmente si tende a indicare un malware come sponsorizzato da uno Stato senza avere abbastanza prove. All'industria della cyber-sicurezza mancano esperti di geopolitica in grado di inquadrare meglio certi episodi, e il risultato è che i report rischiano di essere politicamente deboli e semplicistici. "Le ipotesi sono trattate come fatti; i Paesi considerati come entità monolitiche con motivazioni prevedibili".

Aggiungiamo pure la cautela verso ipotesi che potrebbero non piacere ai clienti della società.

Chi è l'attaccante?

Tutto ciò fa sì che l'individuazione di chi sta dietro a un attacco informatico – processo noto come attribuzione – rischi di essere troppo banale. Ovvero: un'industria del Paese A è stata attaccata; il malware usato presenta delle somiglianze con quello impiegato in altri attacchi condotti da hacker considerati appartenenti al Paese B; i due Paesi non sono in buoni rapporti; il mandante dell'attacco all'industria del Paese A è il governo del Paese B.

"È difficile individuare l'origine di un attacco, specialmente nel caso di Stati", mi spiega Raiu. "Negli ultimi anni molte aziende stanno facendo delle attribuzioni superficiali, del tipo: se a essere colpito è un certo obiettivo, allora concludono che l'attaccante è un Paese nemico, invece di analizzare i dati tecnici. Ma va anche detto che dall'analisi di un attacco è comunque difficile risalire a uno Stato. In genere si individua la lingua usata da chi ha sviluppato il malware, per cui si dice: sono hacker che parlano cinese, o russo, o portoghese, o rumeno e via dicendo. Inoltre in molti casi gli hacker non lavorano direttamente per dei governi, si muovono in modo opportunistico, magari hackerano quello che ritengono importante e rivendono le informazioni. Solo in alcune situazioni si riesce ad arrivare a una attribuzione attendibile, che porta fino agli individui che hanno perpetrato un attacco". Senza contare, prosegue Raiu, che gli Apt sono in evoluzione costante per cercare di non essere individuati.

"È difficile distinguere hacker sponsorizzati da Stati da quelli che non lo sono, ma diciamo che nel primo caso ne sentiamo l'odore", mi dice Eugene Kaspersky, 51 anni, in una pausa delle conferenze di Tenerife. Indossa una camicia hawaiana, e poche ore dopo avrebbe guidato le danze della grande festa conclusiva, vestito da cappellaio magico o qualcosa del genere, uscendo ogni tanto a fumare una sigaretta. Oggi è il 65esimo milionario in Russia secondo la rivista "Forbes", fondatore della più importante società di cyber-sicurezza al mondo secondo la testata americana "Wired"[7], con 300 milioni di utenti in tutto il mondo. E tutto ciò malgrado i suoi forti legami con Mosca: dagli studi, giovanissimo, all'Istituto russo di crittografia, telecomunicazioni e informatica, sotto l'influenza dell'allora Kgb, al periodo passato nell'esercito sovietico come

agente di intelligence, fino alle sue relazioni attuali con la polizia e l'Fsb, i servizi segreti federali per la sicurezza, eredi del Kgb.

Relazioni anche inevitabili, considerato quel che è successo nel 2011, quando dei criminali hanno rapito suo figlio, di 21 anni, chiedendo un riscatto di 3 milioni di euro. In pochi giorni le forze di sicurezza russe si sono mobilitate e alla fine il giovane è stato trovato e liberato, e i sequestratori arrestati[8]. Ad ogni modo, considerata tutta la sua storia personale e famigliare, era probabilmente destino che la sua azienda, da venditrice di antivirus, diventasse una dei leader della cyber-intelligence e della caccia alle spie digitali.

"I criminali cercano in genere dati finanziari, mentre hacker statali puntano a segreti tecnologici, ministeri e ambasciate", prosegue Kaspersky. "Gli Stati che stanno entrando in questo gioco sono sempre di più. E la differenza tra spionaggio e sabotaggio alla fine è solo una questione di 'upgrade', di aggiornamento del software. Nello stesso tempo i gruppi cyber-criminali stanno copiando strumenti, tecnologie, idee avanzate da attori parastatali. Stanno imparando dagli Stati".

Infrastrutture critiche e cyber-guerre fredde

Questa escalation internazionale sul fronte dell'hacking, operata da gruppi statali, parastatali e criminali, sta facendo preoccupare sempre di più chi si occupa di infrastrutture critiche, cioè quel genere di risorse vitali per un Paese industrializzato, come energia, trasporti, sanità, ecc. Mentre nell'aprile 2016 la Nato dava vita a una ambiziosa simulazione di guerra informatica[9], all'incirca negli stessi giorni un attacco importante – e per nulla simulato – andava a colpire proprio dei sistemi industriali europei. Il fornitore di energia elettrica tedesco Rwe, che gestisce la centrale nucleare di Gundremmingen, non lontano da Monaco di Baviera, comunicava infatti di aver trovato delle infezioni su alcuni suoi pc, fortunatamente non collegati a Internet. Il malware – tecnicamente un worm, vecchio e non mirato specificamente alla centrale, il cui obiettivo era rubare credenziali di accesso degli utenti – ci era arrivato tramite chiavetta Usb. Se quindi quel tipo di infezione non era particolarmente preoccupante, era tuttavia poco incoraggiante la facilità con cui era stato veicolato. Del resto erano state proprio delle chiavette Usb, come abbiamo visto, a portare Stuxnet fino

all'impianto di arricchimento dell'uranio di Natanz. Si è trattato di un segnale d'allarme, che però seguiva episodi ancora più inquietanti.

Solo quattro mesi prima, il 23 dicembre 2015, in Ucraina si era registrato un altro attacco dagli effetti senza precedenti. L'hackeraggio della utility dell'energia ucraina Prykarpattya Oblenergo ha tolto la corrente per sei ore a 230mila residenti della regione di Ivano-Frankivsk. Insomma, un cyber-attacco che porta a un blackout energetico, uno degli incubi di chi gestisce infrastrutture critiche.

Gli esperti che hanno analizzato l'aggressione concordano su un fatto: è stata progettata ed eseguita molto bene. Gli attaccanti hanno prima infettato dei dipendenti dell'azienda via mail (attraverso allegati Word), quindi si sono mossi nella rete aziendale fino a ottenere le credenziali dei sistemi di controllo industriale che gestivano la rete elettrica. E mentre staccavano una serie di sottostazioni, lasciando al buio migliaia di ucraini, si premuravano perfino di bloccare le linee telefoniche dell'azienda – e le segnalazioni dei clienti – ingolfandole con finte chiamate. I tecnici del centro di controllo hanno dovuto ripristinare le varie sottostazioni recandosi sul posto, con interventi manuali, perché da remoto non riuscivano più a dare i comandi.

"Dopo l'attacco alla centrale, i suoi operatori per altri due mesi sono andati avanti comunicando attraverso carta e telefono. Tra l'altro i sistemi di protezione che avevano non sono molto diversi da quelli usati in Occidente", mi ha spiegato Andrea Rigoni, advisor Nato e codirettore del progetto CyberDefence in Georgia, dove proprio in quei mesi veniva allestito un centro per difendersi da situazioni di questo tipo. Anche qui, non è un caso: in concomitanza col conflitto con la Russia, nel 2008, la Georgia è stata investita da una serie di attacchi informatici contro i siti del governo, ma anche di aziende, media e trasporti.

Vi presento l'Apt più famoso: Apt28 o Sofacy

L'intelligence ucraina ha subito puntato il dito contro Mosca, anche in considerazione delle tensioni geopolitiche tra i due Paesi. Ma come accade spesso in questi casi, le prove per l'attribuzione di un attacco sono esili e spesso contraddittorie. E dare la caccia all'attaccante è un po' come muoversi in un labirinto di specchi. Alcuni, come l'Istituto americano per

la tecnologia delle infrastrutture critiche, hanno provato a tracciare una mappa degli Apt globali. Ebbene, nella sola Russia ci sarebbero almeno 14 gruppi diversi dediti ad attacchi mirati e persistenti. Alcuni hanno ricevuto dai ricercatori nomi fantasmagorici, da Epic Turla a CosmicDuke. Il più noto e il più attivo, nonché quello che è stato più studiato e attribuito alla Russia se non direttamente al suo governo, si chiama Apt28 (ma ha molti altri nomi, dati di volta in volta da ricercatori e società diversi: è stato battezzato Sofacy, Fancy Bear, Pawnstorm, Sednit e Strontium, il che contribuisce ad aumentare la confusione).

Tra i primi a scoprirlo – e ad attribuirlo al governo di Mosca – sono stati, nel 2014, i ricercatori di FireEye, l'azienda americana già citata sui report relativi ai cinesi. Fondata una decina d'anni fa da un ex ingegnere di Sun Microsystems, Ashar Aziz, si è specializzata nell'individuazione di attacchi informatici avanzati, concentrandosi su un approccio predittivo alla protezione di reti e computer, e usando vari strumenti per riconoscere tentate intrusioni. L'azienda è considerata vicina al governo, alle industrie e ai servizi statunitensi. In-Q-Tel, il fondo d'investimenti tech della Cia, ha scommesso su questa società della Silicon Valley, e ancora oggi ne detiene una piccola percentuale. FireEye ha puntato molto sulla cyber-intelligence anche con una serie di acquisizioni, comprando prima Mandiant, che era specializzata nello spionaggio cinese, e poi la società texana iSight Partners, che ha una rete di oltre trecento analisti in 17 Paesi, impegnati a monitorare gruppi hacker e cyber-criminali infiltrando anche le loro comunità online.

Apt28 o Sofacy è un gruppo d'origine russa tra i più sofisticati. "Si tratta di un gruppo sponsorizzato dallo Stato, che colpisce soprattutto organizzazioni dell'Est Europa, in particolare ministeri degli Esteri. Il suo obiettivo è raccogliere informazioni di intelligence utili per il governo di Mosca", mi spiega Yogi Chandiramani, direttore commerciale per l'Europa e il Mediterraneo di FireEye. "Abbiamo visto che il codice del malware usato dal gruppo era compilato durante le ore d'ufficio del fuso orario di San Pietroburgo".

Sulle finalità di Apt28 concordano diversi analisti. A Kaspersky lo chiamano Sofacy. "È un gruppo longevo, che colpisce obiettivi militari e istituzioni europee. Hanno molti strumenti e risorse, se individui un loro malware nel tuo network dopo poche ore tornano con un altro tipo di

software malevolo. E il loro obiettivo è lo spionaggio a lungo termine", mi spiega Vicente Diaz, ricercatore di punta del colosso di cyber-sicurezza russo. Ma se sull'analisi le diverse società spesso concordano, è sulla attribuzione di attacchi specifici che aumentano le divergenze. E questo è solo uno dei grovigli in cui si muovono anche i più navigati analisti quando devono districare simili assalti informatici. Grovigli che in futuro potrebbero avere conseguenze politiche dirette.

Mentre scrivo, nell'estate 2016, proprio Sofacy (o Apt28) è tornato ancora alla ribalta. La ragione è che alcuni esperti di sicurezza americani hanno additato questo gruppo come il responsabile degli attacchi informatici che hanno colpito, nei mesi precedenti, il Comitato nazionale democratico. Un'operazione che, tra le altre cose, ha portato alla pubblicazione online di oltre 20mila mail sottratte ai "server" dell'organo del Partito democratico. Tutto ciò in piena campagna presidenziale. Con un fantomatico hacker rumeno, Guccifer 2.0, a rivendicare l'azione. Ma soprattutto con lo staff di Hillary Clinton, vari esperti di sicurezza statunitensi e infine anche l'amministrazione americana a puntare il dito contro Mosca.

Ma è stato davvero Sofacy a compiere l'azione? Dobbiamo pensare che il gruppo dedito per anni a un silente cyber-spionaggio abbia iniziato a fare azioni di tutt'altro tipo, da guerra psicologica e propaganda, entrando a gamba tesa nella politica americana? O forse non è stato Sofacy ad agire? In verità, l'unica domanda alla quale valga la pena di rispondere è: ci sono le prove che ad attaccare i democratici siano stati hacker russi per conto del loro governo? Paradossalmente, l'unico che forse potrebbe avere queste prove è il governo americano. Almeno mentre scriviamo, però, non le ha ancora mostrate. O ha deciso di non volerle mostrare, anche perché farlo potrebbe voler dire bruciare a sua volta dei suoi asset.

Il labile confine tra azioni statali e criminali

Il problema è che, in alcuni casi, la natura di alcuni di questi Apt è ibrida. I suoi attori, e le loro azioni, si collocano in un'area grigia fatta di criminalità e legami con operazioni di Stato. La definizione stessa di cosa sia un Apt si basa essenzialmente sull'analisi delle sue tracce e dei suoi strumenti di lavoro. Che possono essere usati da più entità, e rimescolarsi con quelli di

altri.

Per capirlo torniamo alla storia del blackout ucraino. Il malware usato in quel caso si chiama BlackEnergy3, e appartiene a una famiglia di strumenti che sarebbero stati usati da un gruppo (chiamato appunto BlackEnergy) promosso ancora una volta dal governo russo, almeno secondo l'Istituto americano per la tecnologia delle infrastrutture critiche. Dunque l'attribuzione almeno questa volta è chiara? In realtà no. Non per il già citato Diaz, almeno, che si mostra di nuovo scettico, perché "sappiamo poco su chi lo ha effettivamente usato". La ragione di tale scetticismo in questo caso è interessante, poiché ha a che fare col particolare tipo di software malevolo adottato. BlackEnergy è un kit di strumenti impiegato da anni da diverse organizzazioni criminali, spiega un rapporto della società di sicurezza finlandese F-Secure. In pratica è un "crimeware", cioè un tipo di malware progettato per automatizzare delle operazioni criminali, ed è un prodotto realizzato per essere commerciato, e di fatto venduto nell'underground russo della Rete fin dal 2007. La sua modularità e popolarità lo hanno diffuso tra gang diverse, molte delle quali lo usano per rubare credenziali bancarie. Anche se non sono mancati utilizzi politici, come negli attacchi condotti contro la Georgia nel 2008. "L'uso di BlackEnergy per attacchi di natura politica è una intrigante convergenza fra attività criminali e spionaggio", scrive F-Secure. "Poiché il kit è usato da molteplici gruppi, fornisce un maggior margine per sviare possibili attribuzioni".

La convergenza e sovrapposizione di criminali e spie, o quanto meno dei loro strumenti, è un processo bidirezionale. Da un lato gli Stati comprano vulnerabilità informatiche anche dai mercati neri; dall'altro, "quando un certo strumento, un malware in mano a gruppi statali viene scoperto dai ricercatori, allora viene condiviso con cyber-criminali, perché tanto non lo si può più usare, se non rischiando di svelarsi", commenta Chandiramani. "Questa circolazione di strumenti nell'underground confonde gli analisti che indagano su un caso specifico".

Anche perché definizioni e report provano a incasellare realtà molto variegate, dalle appartenenze fluide e dai confini incerti, specie se si finisce nell'ambito della cyber-criminalità. "Apt è un'espressione usata da voi giornalisti; noi siamo un gruppo di russi, attivi da sette anni, anche se non lavoriamo per il governo. Vendiamo vari strumenti e zero-day e abbiamo

una percentuale dalla condivisione di alcune risorse”, mi scrive un hacker russo individuato attraverso il suo sito web, da cui vende, attraverso una grafica quasi corporate, vari tipi di malware. Il sito è collegato a un account Twitter che allude a un’appartenenza a Sofacy, ma non ho potuto verificare tale legame. “Non tocchiamo dati di carte di credito o siti bancari. Diciamo che il nostro è più un hobby. Abbiamo attaccato siti in Germania, Stati Uniti, Svezia, anche se in quest’ultimo Paese ci interessava solo l’azienda dell’energia Vattenfall”.

In effetti, in contemporanea a questa curiosa intervista, sulla stampa norvegese stavano emergendo indiscrezioni su un possibile cyber-attacco subìto in Svezia da Vattenfall, una grossa compagnia energetica del Nord Europa. Nello stesso periodo l’intelligence svedese accusava la Russia di aver mandato in tilt, con un attacco informatico, il sistema di controllo del traffico aereo nei suoi aeroporti per alcuni giorni, nel novembre 2015. Forse l’hacker con cui ho parlato si è intestato un attacco altrui. O forse l’attacco non è mai avvenuto, perché nessuno lo ha potuto davvero verificare.

La questione della corretta identificazione degli autori di cyber-attacchi è così delicata che a fine aprile 2016 la Darpa, l’agenzia per la ricerca avanzata della difesa Usa, ha pubblicato un bando per un progetto di ricerca in grado di migliorare l’individuazione dei responsabili di aggressioni digitali.

Quello che possono fare nel frattempo gli Sherlock Holmes dei virus è cercare di stare ancorati a frammenti di evidenze, da incastrare progressivamente in un puzzle. Così si inizia da un pezzo di malware, dalla mail che lo ha veicolato, si cercano altri campioni simili, o altre vittime, si prova a risalire ai server usati in una certa campagna, si incrociano le informazioni, e si inizia a profilare gli attaccanti. Ovviamente le caratteristiche dei target pesano molto nel valutare chi abbia interesse a prenderli di mira. E contano le armi impiegate: più sono personalizzate, create *ad hoc* e sofisticate – utilizzando anche costosi zero-day, cioè vulnerabilità note solo agli attaccanti –, più l’aggressore è di alto profilo. “Anche se tra gli Apt cresce la pratica di nascondersi dietro strumenti e attacchi di basso livello, che sembrino casuali, per non destare sospetti”, commenta Diaz.

Il risiko statale degli Apt

Ma quali sono i gruppi più dinamici e potenti sulla scena attuale? "Nel 2015 i russi di Sofacy sono stati sicuramente tra i più attivi. Ma non va dimenticato l'americano Equation Group, che però ha diminuito l'attività dopo il nostro rapporto su di loro", dice ancora Diaz. Equation Group sarebbe una sorta di unità d'élite di cyber-spionaggio, con un campo d'azione di almeno 42 Paesi, individuata proprio da Kaspersky nel 2015, e tracciata da alcuni fino all'americana National Security Agency (Nsa).

Di questo gruppo si è tornati a parlare improvvisamente nell'estate 2016, quando, in piena campagna presidenziale americana, con i democratici hackerati da misteriose entità, un gruppo di hacker di nome Shadow Brokers ha messo all'asta una serie di strumenti per compiere attacchi informatici rubati proprio a Equation Group. Dopo il primo sbalordimento, nei giorni successivi, la notizia è stata confermata. I file diffusi dal gruppo per dare credito alla propria asta (che appare essenzialmente una provocazione) contenevano fra le altre cose exploit progettati per bucare i "firewall" prodotti da aziende, anche americane, come Cisco, Juniper, Fortinet e Topsec[10]. Per giorni si è discusso se gli hacker avessero hackerato la Nsa o non piuttosto alcuni server e infrastrutture usati dall'agenzia per attaccare a sua volta, o addirittura se il "leak" (la fuga di dati) non arrivasse da un insider, da un dipendente. Ma l'idea che qualcuno rubi le armi digitali della più potente agenzia di hacking e di intelligence elettronica al mondo e le metta in vendita online con tanto di sberleffi, mentre il Partito democratico americano subisce attacchi informatici e conseguenti imbarazzanti leak di mail giusto poco prima delle elezioni, sembra configurare il fattore scatenante di una tempesta perfetta. Che non promette nulla di buono.

Tra l'altro, ancora nell'estate 2016, Kaspersky e in contemporanea l'americana Symantec hanno pubblicato due report su un nuovo gruppo/campagna di cyber-spionaggio di alto livello, Project Sauron, che sarebbe andato avanti del tutto nascosto da almeno cinque anni. Sebbene le due aziende non si sbilancino a dire chi siano i suoi creatori, i target degli attacchi e il fatto che il malware riprenda molte caratteristiche di Stuxnet e di altri software di spionaggio sofisticati chiamati Regin e Duqu (di derivazione statunitense, britannica e israeliana) fanno sentire odore di

Occidente.

Se i gruppi organizzati di spie e criminali informatici localizzati dalle diverse società di sicurezza in Russia sono numerosi, quelli considerati di area statunitense sono pochi ma potenti. In alcune operazioni, come quella di Stuxnet – che come abbiamo detto è ormai considerata un'azione congiunta Washington-Tel Aviv, con l'aiutino di Londra –, si confondono con Israele. Del resto le potenze in campo sono queste: Usa, Russia, Israele, Cina, Francia, Gran Bretagna e – dato in ascesa – lo stesso Iran. Sulla Corea del Nord – a cui è stato ricondotto il clamoroso attacco alla Sony del 2014 – ci sono pareri contrastanti. Mentre per quanto riguarda la Cina, "dopo l'accordo del 2015 fra Obama e il presidente cinese Xi Jinping per limitare il cyber-spionaggio, abbiamo registrato meno movimento da parte dei gruppi di quel Paese", rileva Diaz. Il che, aggiunge il ricercatore, rischia quasi di essere un problema, dal momento che hacker di Stato "disoccupati" potrebbero riciclarsi tra le file della cyber-criminalità.

Il rimescolamento fra gruppi parastatali e cyber-criminali è la tendenza forse più inquietante indicata nelle analisi degli addetti ai lavori. Anche perché, aggiunge a sua volta Chandiramani, i gruppi Apt a sfondo criminale sono in crescita, e aumentano le gang che cercano soprattutto di ottenere vantaggi economici. Utilizzando mezzi e metodi non molto diversi da quelli degli Stati.

[1] https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

[2] http://www.computerweekly.com/news/2240223685/Industrial-control-systems-increasingly-under-attack-says-Kaspersky.

[3] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, New York 2014.

[4] http://www.zerodaysfilm.com.

[5] Rete di computer infettati e controllati da remoto.

[6] Juan Andrés Guerrero-Saade, *The ethics and perils of APT research: an unexpected transition into intelligence brokerage*, http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf.

[7] http://www.wired.com/2012/07/ff_kaspersky/.

[8] Si dice che da allora si sia rafforzata l'idiosincrasia di Eugene Kaspersky verso i social network, come Facebook e il russo VKontakte, perché qui il figlio avrebbe lasciato troppe informazioni su di sé.

[9] Denominata "Locked Shield" e organizzata tutti gli anni a Tallinn, in Estonia.

[10] I firewall sono sistemi di sicurezza usati per prevenire accessi non autorizzati in una rete.

2.
Mercanti di attacchi

AAA Vendesi vulnerabilità

"La vita è breve. Vendi il tuo zero-day a Zerodium". Così recita il motto di Chaouki Bekrar, uno dei protagonisti di un mercato tanto segreto quanto emergente: quello degli attacchi informatici. Negli ultimi mesi, a dire il vero, questo mercato è già emerso più volte. In alcuni casi, per errore. In altri, volutamente, con i broker di vulnerabilità ed exploit – ossia, come abbiamo visto, codici che sfruttano un baco di un software per lanciare un attacco informatico – che hanno iniziato a farsi una pubblicità inusuale. Proprio come Bekrar.

Facciamo un passo indietro, al settembre 2015. Mentre milioni di persone corrono ad aggiornare i propri iPhone e iPad a iOS 9 – allora l'ultimo sistema operativo di Apple – l'azienda statunitense Zerodium, fondata da Bekrar, esce dall'ombra degli addetti ai lavori e conquista la ribalta dei media mettendo su iOS 9 tre taglie da un milione di dollari l'una. Tre esorbitanti ricompense per chi fosse in grado di fornirgli una tecnica capace di fare "jailbreak" da remoto dei dispositivi Apple, cioè di rompere il sistema di sicurezza degli iPhone e degli iPad e di infettarli senza metterci le mani sopra, utilizzando come vettore di attacco una pagina web visitata dall'utente, un sms ricevuto, o ancora una app del dispositivo. Quelli di Zerodium avevano anche preparato una locandina *ad hoc*, in stile western: "Wanted. Jailbreak per iOS 9. Ricompensa: un milione di dollari".

La cifra stellare, per quanto fosse a suo modo lusinghiera per Apple[11], era però anche un campanello d'allarme. Perché mostrava che esistevano compratori altrettanto stellari. Come le agenzie governative. Non a caso, pochi mesi dopo si assisterà al braccio di ferro tra Apple e l'Fbi (che

vedremo più avanti) per sbloccare un iPhone. Scontro che si concluderà con i federali che avrebbero acquistato misteriosi attacchi informatici da una altrettanto misteriosa azienda per aggirare i sistemi di protezione del colosso di Cupertino. E avrebbero pagato, anche in questo caso, un milione di dollari.

Forse prendendo nota di questo trend, il colosso fondato da Steve Jobs nell'agosto 2016 ha lanciato il suo primo programma di "ricompense per bachi" ("bug bounty"), offrendo fino a 200mila euro per vulnerabilità zero-day trovate da ricercatori sul proprio software. Il problema è che la concorrenza, cioè chi è disposto a pagare per i bug della stessa azienda di Cupertino, è spietata. E disposta a mettere sul piatto molti più soldi.

A distanza di una sola settimana dal lancio del programma di Apple, una società specializzata nel brokeraggio di vulnerabilità ha dichiarato di essere disposta a pagare più del doppio della Mela morsicata. Si tratta di Exodus Intelligence, una delle aziende di spicco del settore, con sede in Texas, che vende informazioni su vulnerabilità ed exploit ad aziende di cyber-sicurezza e governi. "Troviamo il 95 per cento delle nostre vulnerabilità facendo ricerca internamente", mi aveva detto in precedenza il presidente Logan Brown. "Abbiamo anche un programma di acquisizione che non utilizziamo molto. In Exodus lavorano 23 dipendenti, di cui 14 sono dedicati alla ricerca di zero-day". In realtà il loro programma di acquisizione esterno sembra essere cresciuto ultimamente, visto che dall'agosto 2016 Exodus si è messa perfino a comprare exploit via Bitcoin e Western Union, modalità di pagamento spesso predilette dai venditori per mantenere l'anonimato.

Zerodium invece, come abbiamo visto, sugli iPhone aveva piazzato già da prima delle taglie fenomenali. "Vogliamo catturare gli exploit zero-day più avanzati e le vulnerabilità a rischio più elevato che sono scoperte, conservate e a volte accumulate da ricercatori di talento in tutto il mondo", mi aveva detto all'epoca Bekrar via mail. "iOS 9 è il sistema operativo mobile più sicuro in questo momento e sviluppare una catena di exploit in grado di aggirare gli avanzati sistemi di mitigazione [protezione] adottati è un processo lungo e complesso. Per questo abbiamo pensato che un milione di dollari sia una cifra abbastanza alta per motivare molti ricercatori talentuosi". Gli exploit acquistati saranno poi rivenduti ai clienti di Zerodium.

Bekrar e la sua azienda sono tra i protagonisti più di spicco di un mercato in realtà molto opaco e sconosciuto: quello della acquisizione e rivendita di exploit. Una piazza dove si mescolano ricercatori e aziende di sicurezza, governi, broker e cyber-criminali. Fino a poco tempo fa era un mondo connotato dalla segretezza. "Sarà dura trovare qualcuno disposto a parlare", mi aveva detto un esperto del settore. Ora però le cose sono in parte cambiate. E c'è chi ha iniziato a essere volutamente più visibile.

Come Bekrar appunto, che si definisce, con un certo sarcasmo, il Darth Vader della sicurezza informatica, al punto da aver messo la maschera del cavaliere Jedi, sedotto dal Lato Oscuro della Forza di *Guerre Stellari*, come immagine sul suo profilo Twitter. Ma che ha fatto proprie anche alcune definizioni giornalistiche nei suoi riguardi, come il "lupo di Vuln Street", dove Vuln sta per vulnerabilità del software.

Bachi e codici di attacco

Con la sua precedente società, Vupen, che aveva sede a Montpellier in Francia, Bekrar vendeva exploit perfino all'americana Nsa – anche se diceva di usare perlopiù risorse interne nella ricerca di vulnerabilità e nella loro trasformazione in attacchi. Zerodium, fondata successivamente negli Stati Uniti, sarebbe invece più esplicitamente una piattaforma di brokeraggio, un trader che compra exploit in giro e li rivende. A governi, loro contractor, aziende. Una compravendita di codici di attacco e fra questi in particolare i più ricercati e cari, gli zero-day, che come si è già detto sfruttano vulnerabilità del software ancora sconosciute a chi lo ha sviluppato e agli utenti.

Cosa sono le vulnerabilità? Sono dei "bug", dei "bachi", cioè degli errori, dei difetti del codice o della logica di un programma, che possono essere sfruttati per modificarne il corretto funzionamento e quindi per attaccare una applicazione o un sistema. Un esempio di baco di codice: hai un'area di memoria grande 10 byte ma l'utente ce ne può scrivere 11 e causare un "crash", un blocco. Un esempio di baco logico: hai un'app che quando apre un *file.exe* rinominato come un finto pdf te lo esegue: qui lo sviluppatore ha sbagliato la logica e tu puoi sfruttare quel bug a tuo favore per far compiere all'applicazione cose che non dovrebbe fare.

"Esistono varie classi di bug: sicuramente tra le più comuni ci sono quelle

in cui l'input dell'utente non viene controllato adeguatamente oppure viene dato per sicuro. Questi bug possono essere sfruttati per eseguire attacchi. Alcuni sono dei classici come le Sql Injection[12]; queste consentono di eseguire su un database delle 'query' (ricerche) che invece non si dovrebbero poter fare (le Sql Injection sono spesso la fonte dei principali leak online di dati hackerati da siti). Altri attacchi sono più subdoli e appartengono ad errori di tipo logico: ad esempio durante la copia in memoria dell'input di un utente viene sbagliato qualcosa di triviale (banalmente: si inizia a calcolare la lunghezza dei dati da 1 invece che da 0) e quindi il programma finisce per scrivere in posizioni errate della memoria: tali vulnerabilità sono spesso sfruttabili per deviare il flusso di esecuzione di un'applicazione. In pratica si fa fare al programma qualcosa che lo sviluppatore dell'applicazione non aveva previsto e che sicuramente non era sua intenzione veder succedere, come aprire un'immagine che invece scarica un malware. Le categorie sono tantissime, alcune sono più complicate da trovare, altre possono essere devastanti in termini di sicurezza".

A parlare è Alberto Pelliccione, Ceo della società di cyber-sicurezza ReaQta, con sede a Malta. Lui conosce bene questo mercato. È stato il fondatore, nel 1999, di una delle più importanti community italiane dedicate all'analisi di malware; si è specializzato in sicurezza offensiva, un eufemismo per indicare tecniche e strumenti di intrusione, infezione e intercettazione di sistemi informatici; ha lavorato come responsabile dello sviluppo del prodotto su architetture mobili in Hacking Team, società italiana che per anni è stata leader nel mercato internazionale dei "trojan" (da "trojan horse", "cavallo di Troia", software malevoli usati per ottenere l'accesso a un sistema o a un dispositivo) o degli spyware venduti ad agenzie governative per svolgere indagini – e azienda che, insieme ad altre nel suo settore (come FinFisher o Nso), è stata anche al centro di roventi polemiche per il presunto utilizzo improprio dei suoi software da parte di governi illiberali (come vedremo più avanti)[13]. Proprio per questi motivi, qualche anno fa se ne è andato ed è passato a occuparsi soltanto di sicurezza difensiva con una sua nuova azienda. Insomma, conosce direttamente entrambi i lati della barricata, offesa e difesa. I quali, come riconoscono tutti i maggiori esperti di sicurezza informatica, sono in realtà strettamente intrecciati: un aspetto che ha delle implicazioni sottili qualora si voglia

provare a regolamentare alcune di queste attività, come il commercio di exploit.

Ma torniamo ai bachi. Quando gli sviluppatori vengono a conoscenza di un bug in un software, rilasciano un aggiornamento dello stesso in cui l'errore viene corretto. In inglese si usa il termine "patch", "pezza", che nasce dalle correzioni "fisiche" effettuate con ritagli sui nastri o sulle schede perforate dei calcolatori degli anni Cinquanta. I computer si sono evoluti, i bachi sono rimasti.

"I bug diminuiscono mano a mano che vengono 'patchati', ma il software è sempre in sviluppo, per cui nuovi bug vengono aggiunti", prosegue Pelliccione. "Ciò avviene principalmente in tre modi: scrivendo nuovo codice, per cui si possono involontariamente aggiungere anche vulnerabilità; facendo 'refactoring' del codice già esistente, cioè in sintesi modificandone la struttura per ottimizzarlo; o attraverso sviluppatori che lo facciano volutamente, pagati da qualcuno (un'agenzia di intelligence, ad esempio)".

Se poi qualcuno trova una vulnerabilità in un software, ha in sostanza tre possibilità: può avvisare gli sviluppatori; può creare un codice di attacco (exploit) in grado di sfruttarla e quindi utilizzarlo; oppure può rivendere la vulnerabilità o il relativo exploit a qualcun altro. Gli exploit zero-day sono i più costosi perché colpiscono le vulnerabilità che nessuno ancora conosce, tranne gli attaccanti che le hanno scoperte o che le hanno comprate da altri. Ma ci sono anche moltissimi exploit che colpiscono vulnerabilità già note che però non sono state ancora corrette dagli sviluppatori; oppure lo sono state, ma gli utenti non hanno aggiornato il software. Non sono più tecnicamente zero-day, ma vengono definiti "n-days": sono cioè trascorsi "n" giorni dalla divulgazione della falla, invece che zero. Ma possono essere ugualmente molto efficaci. "Tutti i gruppi cyber-criminali corrono a creare exploit appena è pubblicata una vulnerabilità. Gli utenti inizieranno ad aggiornare i sistemi solo dopo il rilascio delle patch. Cosa che può avvenire a ore, giorni o anche mesi di distanza dalla pubblicazione dei dettagli della stessa falla", commenta ancora Pelliccione. "A correre a fare exploit su una vulnerabilità appena resa nota sono anche molte aziende che poi li rivendono ad altre che fanno 'pen testing'", vale a dire ad esperti che sono pagati per sondare le difese di grosse imprese attaccando i loro sistemi o applicazioni – cioè facendo test

di penetrazione (penetration testing).

Dai supermercati dell'hacking alle boutique per governi

Il mercato degli exploit è un mondo fatto a strati. Alla base c'è il mercato nero e perlopiù criminale. Comunica su forum online ad accesso riservato, come il celebre Darkode, in passato sequestrato dall'Fbi. E su tanti siti minori, come 0day.in, che stanno alla luce del sole, anche se limitano l'accesso degli iscritti. Anche sui siti delle "darknet" – reti dove sia chi gestisce siti e servizi sia i loro utenti sono protetti da anonimato – ci sono scambi del genere, con gli annunci dei venditori e i feedback dei compratori. È un po' l'outlet di questo settore: si trovano vulnerabilità economiche, a volte usate, e non mancano le fregature. Sul mercato nero AlphaBay nel 2015 un tizio vendeva uno zero-day per pdf in grado di scaricare ed eseguire un programma malevolo sul computer di una persona: bastava che questa aprisse il pdf infetto. Era venduto a 2500 dollari. Lo stesso venditore offriva uno zero-day per il browser Tor per quattromila dollari. Una cifra non molto alta – considerato il tipo di exploit – perché funzionava su versioni vecchie del browser, e quindi solo contro utenti che non lo avevano ancora aggiornato. La quantità di target contro cui si può utilizzare è infatti una delle variabili che determinano il valore di uno zero-day.

Risalendo la scala di questo mercato, in cima si trovano invece le boutique di lusso che lavorano principalmente con i governi, i loro contractor o grosse aziende. Società come Zerodium, appunto. O Exodus Intelligence. O Immunity. O ReVuln, piccola azienda fondata da italiani. Molti dei broker o venditori più noti e ufficiali sono americani o fanno affari negli Usa. Il governo statunitense è infatti il primo compratore di exploit. Nel 2013 l'Nsa ha stanziato 25,1 milioni di dollari per "acquisti segreti di vulnerabilità software" da venditori privati, corrispondenti a una stima minima che va dalle 100 alle oltre 600 vulnerabilità all'anno. Dati che sono emersi con i documenti rivelati da Edward Snowden. Dopo gli Stati Uniti, gli altri principali acquirenti di exploit sono Israele, Gran Bretagna, Russia, India e Brasile, oltre ad alcuni servizi segreti mediorientali e la Corea del Nord, secondo le ricerche del Center for Strategic and International Studies di Washington.

Le aziende che sviluppano software hanno provato ad arginare il fenomeno offrendo loro stesse delle ricompense per i i propri bachi: Microsoft, Mozilla, Facebook, Google e più recentemente – come abbiamo visto – Apple hanno tutte lanciato dei bug bounty. Esistono anche dei programmi di acquisizione come Zero Day Initiative – lanciato già nel 2005, poi gestito da Hp e successivamente acquisito dalla società Trend Micro – che paga i ricercatori per individuare bachi riportati poi ai produttori. Oppure HackerOne. Si parla di due, tre, cinque, diecimila dollari a seconda della tipologia. In casi particolari ci si spinge più su, come con Apple. E tuttavia questo sistema non sembra riuscire a competere, sul piano puramente economico, quanto meno con il mercato grigio, fatto di broker e aziende che rivendono nell'ombra ai governi o ad altri attori pieni di risorse.

A questi livelli – quelli dei governi e dei loro contractor e broker – girano molti soldi. Bekrar negli ultimi mesi ha deciso di essere molto esplicito e di tagliare le gambe al cosiddetto mercato bianco, quello alimentato da aziende come Microsoft e Apple per aumentare le proprie difese. Nel giugno 2015 Google pubblica un post in cui fa il punto sul suo programma di ricompense per vulnerabilità trovate da ricercatori esterni su Android, il sistema operativo per dispositivi mobili. In un solo anno "abbiamo pagato 550mila dollari a 82 individui, per una media di 2200 dollari a ricompensa e 6700 a ricercatore. Il più pagato è stato un individuo che ha riportato 26 vulnerabilità incassando 75.750 dollari. Quindici ricercatori sono stati pagati oltre 10mila dollari".

I toni sono orgogliosi, il colosso annuncia di voler pagare cifre più consistenti in futuro. Ma quando questo post viene pubblicato, Bekrar/Zerodium lo cita immediatamente e scrive: "Google paga 30mila dollari per una Rce [Remote Code Execution, una vulnerabilità di sicurezza che permette a un attaccante di eseguire del codice da remoto, la regina nelle tipologie di vulnerabilità perché consente di fare attacchi attraverso Internet]. Noi paghiamo fino a 100mila dollari per una Rce". Nei giorni successivi, twitta nuovamente: "Un ricercatore indipendente ha guadagnato 205mila dollari in un solo mese sottoponendoci tre exploit zero-day". O ancora: "Infastidito dai programmi di bug bounty solo su invito? [il riferimento qui è a quello lanciato poco prima da Apple e limitato solo ad alcuni ricercatori] Non preoccuparti, le nostre GROSSE

ricompense sono aperte a tutti, in qualsiasi momento". E un altro tweet: "Siamo sempre alla ricerca di ricercatori da assumere. Da noi avrete un salario fisso più un bonus tra i 10mila e i 100mila dollari per OGNI exploit che fate".

Zerodium pubblica anche una tabella che mostra come funziona il processo di acquisizione. "Scopri una vulnerabilità zero-day e ne ricavi un exploit. Sottoponi i dettagli tecnici minimi a Zerodium. Zerodium conferma il suo interesse e manda una pre-offerta. Tu ci mandi tutti i dettagli tecnici e l'exploit. Noi ti facciamo l'offerta finale. Tu accetti e sei pagato in una settimana". Tutto spiegato bene, in una infografica.

"Sì, funziona più o meno così", conferma Pelliccione. "Quando tu hai uno zero-day tendenzialmente non vuoi dirlo troppo in giro, dove sta e di cosa fa parte, specie ai broker. Ma nello stesso tempo il broker lo deve sapere, altrimenti non può dirti quanto può pagarti. Quindi il procedimento è che tu dai alcune informazioni minime di categoria, e loro ti danno un prezzo. Per esempio: 'Ho un exploit per Office che viene attivato in fase di visualizzazione di un'immagine presente nel documento e non richiede l'utilizzo di macro'. Poi tu glielo mandi e cerchi di trovare un accordo sul pagamento".

Trattative sotto banco

La compravendita di exploit è un'attività artigianale. Variano i prezzi, le modalità di contrattazione, i termini di pagamento, ma soprattutto l'affidabilità dei soggetti coinvolti. Come fa un compratore a sapere che lo zero-day che sta acquistando in esclusiva e a caro prezzo da un hacker lontano mille miglia non verrà venduto sotto banco anche ad altri? In fondo si tratta di un software che può essere riprodotto e rivenduto innumerevoli volte. "La struttura dei pagamenti è in genere dilazionata in blocchi ed estesa in modo che se la vulnerabilità è scoperta poco dopo l'acquisto, il compratore non deve pagare il prezzo intero", mi ha spiegato Vlad Tsyrklevich, un ricercatore di sicurezza che ha mappato una parte del mercato di exploit. Un mercato, mi dice, basato sulla segretezza. "La maggior parte delle aziende coinvolte non parla volentieri delle proprie attività".

In compenso, lo scouting di talenti e risorse è continuo, diffuso, capillare.

Le occasioni per i venditori in aumento. “Quando inizi a pubblicare vulnerabilità in maniera legittima, inizi ad essere bombardato da strane mail di gente che ti offre dei soldi”, mi ha raccontato Luca Carettoni, che vive all’estero dove guida un team di cyber-sicurezza per una nota azienda di Internet.

Un mercato non regolato

Gli exploit zero-day possono essere usati per potenziare un’arma digitale come Stuxnet, usata in sofisticate operazioni di spionaggio o di sabotaggio interstatale; possono essere impiegati da cyber-criminali interessati a depredare i conti di aziende; possono essere utilizzati dalla polizia per riuscire a infettare con uno spyware lo smartphone di un sospetto criminale nel corso di un’indagine; possono essere adoperati dai servizi di intelligence di un Paese non democratico per infettare e spiare giornalisti, attivisti, avvocati.

Per queste e altre ragioni gli spyware sono diventati oggetto di dibattito politico. Qualcuno, infatti, vorrebbe considerarli delle armi digitali e provare a regolamentarne il commercio. A fine 2015 l’Europa ha concluso una consultazione pubblica[14] per aggiornare la legge sulle esportazioni che regola il commercio di beni a uso duale, ovvero quei prodotti che possono essere usati sia per scopi civili e commerciali che militari. Se un bene è di uso duale richiede una licenza per l’esportazione fuori dall’Europa. Nel 2014 nella lista di questi prodotti sono finiti anche gli spyware. Per parlamentari europei come l’olandese Marietje Schaake, “i diritti umani devono essere inclusi come un criterio di controllo nella legge sulle esportazioni”.

Ma che fare invece con gli exploit? Dovrebbero essere regolamentati? È possibile farlo? Ed è auspicabile? La maggior parte dei ricercatori di sicurezza sono contrari a una loro regolamentazione, anche quando sono favorevoli a normare invece le esportazioni degli spyware o dei trojan. La ragione è semplice: mentre uno spyware ha una funzione e un utilizzo ben specifici, un exploit può essere usato in molteplici contesti. Perfino Bekrar con me ammette che sì, “gli spyware sono decisamente delle armi digitali. Tuttavia gli exploit possono essere sviluppati anche per ragioni di difesa, per fare dei penetration test, e quindi devono essere esclusi da simili

regolamentazioni". Dello stesso parere è Logan di Exodus: "Penso che restrizioni governative interferirebbero solo con la ricerca a scopo di difesa, mentre non avrebbero effetti sul mercato nero delle cyber-armi". Ovviamente loro sono parte interessata. Ma anche chi lavora nella sicurezza difensiva raggiunge conclusioni simili.

Un'idea è dunque provare a spingere il mercato "bianco", quello alimentato dalle aziende tecnologiche disposte a pagare delle ricompense a chi trovi falle sui loro prodotti. "Devi tirare dentro le aziende produttrici di software e hardware", mi dice Carettoni. "E quindi fare in modo che chi lavora nel settore abbia delle compensazioni decorose. Se crei delle alternative valide, le persone inizieranno a considerare quell'opzione". Nel frattempo, però, governi e loro contractor stanno ammassando vulnerabilità ed exploit che tengono per sé, nascoste. C'è un problema di domanda da parte degli stessi Stati. In uno scenario in cui i conflitti anche nazionali si stanno trasferendo in Rete, non è chiaro come fermare una crescente corsa agli armamenti digitali. Nessuno vuole rimanere indietro. A tutto ciò si aggiunge lo spauracchio di terrorismi e di instabilità economico-politiche, per cui anche al loro interno i singoli Stati rivendicano la necessità di avere gli strumenti adeguati per indagare o prevenire attentati e in alcuni casi perfino rivolte. Ma ogni vulnerabilità tenuta sotto banco è un baco che qualcuno nel mondo può sfruttare a discapito di altri. Spesso, a discapito degli utenti, delle aziende, della sicurezza della Rete. "È chiaro che se i governi hanno informazioni su sistemi vulnerabili, che magari riguardano milioni di dispositivi, e non li risolvono, lasciano Internet insicura", commenta Carettoni.

"La ricerca degli zero-day non può essere fermata, e non lo sarà mai perché gli interessi in gioco oggi sono immensi", dice Pelliccione. "Uno zero-day potenzialmente può avere lo stesso valore che per un'agenzia di intelligence ha un asset inserito ad alto livello all'interno di un governo 'nemico' e i costi sono in confronto bassissimi. Acquisire un asset ti costa milioni e impiega anni, un exploit ti costa una frazione e sei dentro nel giro di minuti".

[11] Lusinghiera perché significava che queste vulnerabilità sono molto rare/scarse. E quindi, seguendo la legge di mercato, molto costose.

[12] Sql (Structured query language) è un linguaggio di programmazione usato per comunicare con un database. In un attacco di Sql Injection l'attaccante cerca di "convincere" l'applicazione a eseguire del codice Sql che non dovrebbe eseguire. Per farlo l'attaccante digita dei comandi Sql con l'intento di ottenere l'accesso a dati nascosti.

[13] Dell'industria di spyware ho scritto molto nella mia attività di giornalista. Sulla storia di Hacking Team rimando all'ebook *Attacco ai pirati. L'affondamento dell'Hacking Team: tutti i segreti del datagate italiano*, La Stampa, Torino 2015, scritto con i colleghi Stefano Rizzato, Bruno Ruffilli, Massimo Russo e Raphaël Zanotti.

[14] http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190.

3.
Mi vendo il tuo database (e i tuoi tradimenti)

Se il personale diventa pubblico

“Quando sono tornata dal lavoro, ho notato qualcosa di strano in casa, cose che non erano al loro posto, e poi l’ho scoperto. È stato un momento a cui la vita non ti prepara. Come spieghi ai tuoi figli che il loro padre è morto e che si è ucciso?”.

È molto composta Christi Gibson mentre racconta alle telecamere l’episodio più drammatico della sua vita. Pochi giorni prima, il 24 agosto 2015, suo marito John Gibson, 56 anni, pastore battista e insegnante in un seminario a New Orleans, si è suicidato lasciando un biglietto rivolto alla moglie e ai loro due figli. “Scriveva della sua depressione. E del fatto che il suo nome fosse lì, e di questo era molto molto affranto”, prosegue la donna parlando alla Cnn, aggiungendo che il marito temeva anche di perdere il lavoro. Accanto a lei siedono i due figli adulti. “Tutto quello che sappiamo è che ha speso la sua vita per aiutare gli altri, ha offerto perdono, preghiera e indulgenza a tutti, ma per qualche ragione non ha potuto estenderli a se stesso”.

Il posto dove era finito il nome di John Gibson era online. Era il database che conteneva tutti gli utenti del sito Ashley Madison, trafugato e messo in Rete da uno o più hacker. Anche lui, come altri milioni di persone nel mondo, si era iscritto tempo prima. “La vita è corta. Fatti una scappatella”. Così recita il motto della piattaforma, che è un sito di “dating”, di rimorchio online, uno come tanti, ma che si indirizza soprattutto a una certa tipologia di persone: chi è in cerca di avventure extraconiugali. Ce ne sono diversi di siti del genere, e ogni estate le caselle di posta dei giornalisti

sono inondate dai loro comunicati stampa che elencano classifiche delle città più infedeli o delle ragioni dell'adulterio. Il loro marketing è piuttosto aggressivo, con frasi come: "Il sito della scappatella sicura per persone sposate o impegnate", e via dicendo.

"Cari uomini, prestate attenzione alle donne nate sotto il segno dei Gemelli", recitava nel 2012 un comunicato in italiano proprio di Ashley Madison. Un colosso nel suo campo, fondato in Canada già nel 2002. Il suo modello di business si basa su un misto di iscrizioni gratuite e di messaggi privati a pagamento. A pagare sono gli uomini, da sempre la componente maggioritaria (e a volte con maggioranze bulgare) degli iscritti a questo genere di siti. E cancellare un profilo, una volta aperto, richiedeva comunque una somma di 19 dollari.

Fin qui semplice business, dunque. Almeno fino al 19 luglio 2015. La sera prima, Brian Krebs, noto giornalista tech investigativo, sta al pc in pigiama a casa sua, in Virginia, quando una delle sue fonti anonime gli manda una soffiata. Si tratta di alcuni link ad ampie quantità di dati che sembrano essere stati sottratti dai server di Avid Life Media, l'azienda canadese che gestisce Ashley Madison e altri siti di dating. Krebs vede i nomi degli iscritti, i loro indirizzi, i numeri delle carte di credito. Ci sono anche molti documenti aziendali, che includono il cellulare dell'amministratore delegato di Avid Life Media, Noel Biderman. Krebs gli telefona e Biderman gli conferma che sì, sono stati hackerati, ma che stanno facendo il possibile per far sparire dalla Rete – con delle richieste di rimozione – il materiale con i dati.

Purtroppo per i loro utenti non ci riusciranno veramente. Poche ore dopo, Krebs sul suo blog dà la notizia di quanto sta avvenendo. "Ampie copie di dati rubati dal sito di tradimenti AshleyMadison.com sono state pubblicate online da un individuo o un gruppo che dice di aver completamente compromesso il database utenti dell'azienda, i suoi documenti finanziari e altre informazioni proprietarie. Il leak [la fuga di dati] ancora in corso potrebbe essere molto dannoso per alcuni dei 37 milioni di iscritti", scrive Krebs. Quanto dannoso si capirà solo successivamente. Per ora gli hacker – che si fanno chiamare The Impact Team – provano a ricattare l'azienda se questa non manderà offline i suoi siti di incontri, a partire da Ashley Madison. "Peccato per quegli uomini, sono spregevoli traditori e non meritano discrezione", scrivono gli hacker.

“E peccato per Avid Life Media, non avete mantenuto la vostra promessa di segretezza. Abbiamo tutti i profili degli iscritti e li rilasceremo presto se Ashley Madison rimane online”.

La motivazione degli aggressori è confusa e anche contraddittoria. Da un lato sarebbe una punizione per il comportamento dell’azienda verso gli utenti, poiché diceva di cancellare i profili (a pagamento) senza farlo veramente, scrive The Impact Team. Dall’altro non sembra però esserci alcuna remora né compassione, ma semmai disprezzo, per gli iscritti che rischiano di essere le vittime collaterali della pubblicazione dei dati. “Sembrano motivati dall’immoralità dell’adulterio”, scrive in quei giorni l’esperto di sicurezza Rob Graham. “Ma molto probabilmente la loro prima motivazione è il divertimento, e la seconda il fatto che semplicemente potevano farlo”.

Il sito non va offline come richiesto, e alcuni giorni dopo gli hacker decidono di pubblicare in Rete – nelle darknet, dove non funzionano le richieste legali di rimozione – tutto il database utenti, che include nomi, indirizzi, carte di credito, telefoni e preferenze sessuali di circa 33 milioni di iscritti. È il 18 agosto, che sarà ricordato come il giorno in cui un attacco hacker ha colpito in faccia milioni di utenti comuni, denudando la loro vita privata nemmeno fossero star di Hollywood[15]. Solo che in questo caso i famosi quindici minuti di celebrità si sono incarnati nel peggiore dei reality.

Nelle darknet (definite spesso sui media come Dark Web) i dati sono comunque molto difficili da trovare per la maggior parte delle persone. Ma il giorno dopo affiorano anche sul web detto in chiaro, quello visibile e raggiungibile da tutti. Intanto, tra il 20 e il 21 agosto, gli hacker pubblicano anche i contenuti delle mail di Biderman. Invano Avid Life Media cerca di fermare la diffusione del leak con delle richieste di rimozione per violazione del copyright ai siti o ai profili Twitter che linkano ai dati. È come fermare uno sciame di mosche colpendole una a una con la paletta. I file si scaricano da più parti, basta aprire un client per BitTorrent.

Una marea di dati molto personali

Di quanti e quali dati stiamo parlando per la precisione? Dieci gigabyte di dati compressi. Per dirla con Dave Kennedy, un ricercatore di sicurezza

che è stato tra i primi ad analizzare il "dump" (cioè l'atto di copiare e scaricare da un sito dati, tabelle, ecc.): "Per chi non se ne rende conto, si tratta di una cosa imponente. Enorme". Dove "gli attaccanti hanno mantenuto per tanto tempo l'accesso ai server di Ashley Madison, e a gran parte dei suoi documenti e database, senza che nessuno se ne accorgesse". Il risultato è la pubblicazione di dati personali e di password di 33 milioni di profili – anche se per fortuna sono cifrate, in gergo "hashed". Tra le informazioni sui profili, ci sono quelle sull'aspetto fisico (altezza, peso, ecc.) e sulle preferenze sessuali: "uomo impegnato cerca donna", "uomo cerca uomo", ma anche "dominante/master", "sottomesso/schiavo", "bondage" e simili. Molti dei profili sono falsi, ma anche così ne restano milioni aperti da persone reali. Gli indirizzi fisici spesso sono falsificati, ma a volte sono rimaste in memoria le coordinate Gps, nota ancora Graham. Che aggiunge: ben 28 milioni di profili sono di uomini. Su questo dettaglio torniamo dopo.

Naturalmente nel leak ci sono anche una montagna di documenti corporate sull'azienda – contratti, memo, "chart" dell'organizzazione, tecniche di vendita, mail del management –, ma in questa storia sono quelli che interessano meno. Qualcuno comincia ad analizzare in massa gli indirizzi mail: 15mila appartengono a domini di primo livello del governo o dei militari statunitensi, come *.gov* o *.mil*. Il Pentagono apre un'indagine. Chi è iscritto con l'indirizzo lavorativo comincia ad avere paura di ripercussioni.

Sulle prime tracce

Intanto Avid Life Media e le autorità cercano disperatamente di reagire. L'azienda mette una taglia, offrendo 500mila dollari canadesi (340mila euro) di ricompensa a chiunque fornisca informazioni utili per identificare gli attaccanti. Proprio sull'attacco emergono ulteriori dettagli. Il 25 agosto la polizia di Toronto tiene una conferenza stampa e tra le altre cose consegna ai giornalisti stupiti un foglio con il testo di una canzone. Si viene infatti a sapere che il 12 luglio, pochi giorni prima che Krebs venisse allertato della diffusione dei primi dati, gli impiegati di Toronto di Avid Life Media, al momento del login nei loro computer, si erano trovati davanti il messaggio minaccioso degli hacker, con la loro richiesta di

chiudere i siti, accompagnato dalla musica di *Thunderstruck*, una hit degli anni Novanta della band australiana AC/DC. Vedremo poi che, per quanto bizzarro possa sembrare, proprio la canzone diverrà anche una pista investigativa. Non solo: le autorità canadesi arrivano al punto di rivolgersi direttamente alla comunità di hacker del Dark Web, non esattamente il genere di alleato delle forze dell'ordine. "Vi chiediamo di fare la cosa giusta e contattarci", è l'appello surreale del questore di Toronto Bryce Evans.

Ma la conferenza stampa della polizia non ha solo note di colore. Ci sarebbero indagini in corso su almeno due suicidi che potrebbero essere connessi al leak, spiega lo stesso Evans. Negli Stati Uniti, un capitano della polizia di San Antonio, i cui dati erano nel dump, si toglie la vita. Il 24 agosto, come abbiamo visto all'inizio, si uccide John Gibson. Pochi giorni dopo, l'amministratore delegato Noel Biderman si dimette.

L'arrivo dei piranha

A peggiorare la situazione, nel giro di pochi giorni inizia a svilupparsi un'economia criminale fatta di tanti piccoli piranha che cercano di addentare un pezzo della preda. Sbucano siti come Ashley.cynic.al e Trustify che consentono di fare una ricerca su un indirizzo mail per vedere se faccia parte del leak senza doverselo scaricare tutto. Gli esperti però consigliano di evitarli, perché potrebbero raccogliere e riutilizzare proprio quelle informazioni riservate che si teme siano state diffuse. In particolare, il ricercatore di sicurezza Troy Hunt rileva come Trustify mandi delle mail a persone il cui indirizzo sia stato cercato da qualcuno nel proprio motore di ricerca, per poi offrire "consulenze".

L'esercito degli "spammer" e dei "phisher" inizia a scaldare i motori, facendo partire mail sul tema Ashley Madison per far abboccare utenti particolarmente curiosi o impauriti. Tom Kellerman, dell'azienda di sicurezza Trend Micro, mette subito in guardia dalle torme di truffatori, impegnati a creare mail provenienti da finti rappresentanti di Ashley Madison, o da finti avvocati e studi legali, per tentare di ingannare gli utenti che pensino di essere coinvolti nella diffusione dei dati. E infine, in modo più mirato, si muovono gli estorsori. Purtroppo su quest'ultima categoria esistono varie testimonianze.

"Ciao, ti sto ricattando", esordiva una mail ricevuta da un uomo di 65

anni del Nebraska, sposato. Aveva usato il sito per incontrare tre donne, ma non era andato più avanti di un pranzo insieme. "Se vuoi mantenere segrete le tue bugie e i tuoi tradimenti al tuo partner, alla tua famiglia, ai tuoi amici e al tuo datore di lavoro fai molta attenzione. Poiché quello che chiediamo non è negoziabile e può rovinarti la vita". La mail chiedeva un pagamento di tre bitcoin e, anche se all'inizio la vittima non sapeva neanche cosa fossero, alla fine ha pagato cinque bitcoin (del valore di circa 1000 dollari all'epoca), sperando di togliersi i ricattatori di torno. In realtà ha continuato a ricevere mail di questo tipo per mesi. La storia l'ha raccontata la giornalista Kristen Brown, che ha intervistato un centinaio di vittime del leak. La sua indagine non lascia dubbi sull'impatto psicologico e materiale lasciato dalla vicenda su moltissimi iscritti al sito, trovatisi in un turbinio di incertezza, sensi di colpa, paure, paranoia e ricatti.

Tutto quello che aveva Brown erano indirizzi mail e numeri di telefono di persone finite nel leak. E così la giornalista ha iniziato a scrivergli. "Ho deciso che avrei usato la mail per contattarli, perché avrebbero potuto più facilmente ignorarmi nel caso non se la sentissero di parlare. Nei primi giorni ho scritto a circa duemila utenti di Ashley Madison. All'inizio mi ha risposto qualche dozzina: erano spaventati e confusi riguardo a quello che l'attacco informatico poteva significare per loro. Molti erano anche sollevati di poter parlare con qualcuno che potesse spiegargli cosa stava succedendo. Altri mi hanno rivolto domande sulla loro situazione personale, e ho cercato di rispondere come potevo". Dopo aver pubblicato la sua storia, Brown ha ricevuto poi molte altre mail. "Volevano sapere cosa dovevano fare se qualcuno provava a ricattarli; altri volevano solo sfogarsi. Un tipo ha continuato a scrivermi per mesi: anche se aveva usato una mail finta e una carta di credito usa e getta, temeva che la moglie lo venisse a sapere e io ero l'unica persona a conoscere il suo segreto e con cui poteva confidarsi. In tutto avrò parlato con più di cento persone".

Il ricercatore Toshiro Nishimura ha individuato una vera campagna di estorsioni al riguardo, con una mail che diceva così: "Purtroppo i tuoi dati sono stati 'leakati' nel recente hack di Ashley Madison e ho le tue informazioni. Ho anche usato il tuo profilo utente per trovarti su Facebook, così ora ho una linea diretta per contattare tutti i tuoi amici e la tua famiglia". La mail proseguiva con la richiesta di pagare entro tre giorni 1,05 bitcoin (all'epoca circa 243 dollari) su uno specifico indirizzo. In

pratica l'estorsore si era scaricato il leak, aveva estratto gli indirizzi mail, aveva generato un indirizzo bitcoin per ogni vittima e aveva inviato le mail di ricatto. Questa campagna ha dato i suoi frutti? Sì, secondo Nishimura, che ha provato a rintracciare le transazioni bitcoin inviate dalle vittime sulla base delle quantità richieste. In quattro giorni gli estorsori di questa specifica campagna – non l'unica evidentemente – avevano incassato 6400 dollari.

Ma non ci sono solo i criminali. A peggiorare la situazione, molti giornali locali e blog, specie negli Usa, iniziano a pubblicare i nomi dei residenti che usavano il sito, incuranti tra le altre cose del fatto che chiunque avrebbe potuto inserire la mail di qualcun altro per il processo di iscrizione iniziale, dal momento che gli indirizzi mail non erano validati (diverso ovviamente il discorso per chi aveva comprato i servizi del sito pagando con la propria carta di credito).

Nella cosiddetta Cintura della Bibbia, nel Sud degli Stati Uniti, giornali locali come "The Henry County Report", in Alabama, hanno pubblicato la lista di nomi, indirizzi mail e recapiti delle persone della zona che erano iscritte al sito. "Fedifraghi smascherati!", era il tenore dei titoli. E mentre un sindaco dell'Alabama veniva costretto a dimettersi dopo essere stato indicato tra gli utenti, altri abitanti di questo Stato, "googlando" il loro nome, lo ritrovavano nella suddetta lista, esposta al pubblico ludibrio. "Abbiamo deciso che era interesse dei nostri lettori avere pieno accesso ai nomi degli individui della nostra area", scriveva "The Henry County Report", aggiungendo di aver pubblicato solo gli iscritti paganti. Brown mi ha raccontato di essere stata contattata proprio da un uomo in Alabama, terrorizzato dall'idea di poter essere pubblicamente e virtualmente linciato dai vicini di casa e dalla comunità se si fossero accorti che era iscritto ad Ashley Madison.

Del resto, account Twitter come @KentuckyAMleak hanno perfino twittato (prima di essere sospesi) i nomi di utenti del Kentucky, menzionando dove possibile i rispettivi datori di lavoro. In occasione del leak di Ashley Madison si è visto anche questo: una santa e assurda alleanza tra fanatici religiosi, moralizzatori d'ogni fede e troll internettiani per vergare una riedizione digitale della *Lettera scarlatta*.

Alla ricerca di aiuto e risposte

"Il leak di Ashley Madison è stato certamente il più dannoso per la natura altamente sensibile dei dati e l'ampia pubblicità che lo ha riguardato", mi spiega via mail il già citato Troy Hunt, che di fughe di dati se ne intende. Ricercatore di sicurezza di Microsoft di giorno, di notte gestisce un sito, Have I been pwned?, che raccoglie i dati di siti che sono stati hackerati e successivamente diffusi. In questo modo permette agli utenti di verificare se il loro indirizzo mail sia presente in uno dei tanti leak, in modo da correre ai ripari. Ma l'hackeraggio del sito di relazioni extraconiugali lo ha letteralmente travolto. "Ho reso rapidamente i dati ricercabili da parte di coloro che erano stati colpiti dal leak e ho impostato dei controlli di sicurezza e privacy per fare in modo che solo i diretti interessati – cioè i reali proprietari di un indirizzo mail – e nessun altro potessero trovare il proprio account. Appena fatto tutto ciò, ho iniziato subito a essere inondato di mail – a volte centinaia al giorno – di persone che cercavano di capire cosa stesse succedendo. Erano spaventati da quello che non sapevano – in particolare quali loro informazioni esattamente fossero state diffuse – e dalle reazioni che avrebbero potuto avere i loro partner, i colleghi e la comunità".

Ma non lo contattavano solo per avere assistenza a livello pratico. Molti gli raccontavano spontaneamente perché si erano iscritti, che cosa avevano fatto o meno, e soprattutto gli confidavano le loro attuali paure. Anche in questo caso, come già avvenuto per gli attacchi sponsorizzati da Stati, si creano situazioni che i ricercatori di sicurezza normalmente non sono abituati a gestire, trovandosi ad assolvere ruoli nuovi, perché lasciati ancora vacanti dal resto della società. "Mi pento di essermi iscritto al sito e ora sono terrorizzato dal fatto che potrei fare del male a chi amo e mi sta vicino", gli scrive un utente. Molti anche quelli che gli dicono di non vivere più serenamente: "Sto malissimo. Non posso dormire né mangiare e per di più sto cercando di nascondere a mia moglie che c'è qualcosa che non va". Moltissimi quelli che dicono di essersi iscritti per noia o per gioco, di non averlo mai usato, di aver trovato lì il proprio indirizzo mail anche se non si erano iscritti, di averlo fatto in un particolare periodo della propria vita, o quando erano single e così via.

Un'ampia gamma di sfumature, ragioni e contesti appiattiti in un database

buttato online in pasto alla curiosità morbosa di benpensanti, al "clickbaiting" dei media, all'opportunismo di criminali. Ma Hunt – che ha descritto le tipologie di mail ricevute in un post sul suo blog[16] – sottolinea anche quante persone non avessero piena consapevolezza del funzionamento del sito e più in generale di Internet.

A caccia di Impact Team

Nel momento in cui scrivo, a un anno di distanza dal leak di Ashley Madison, non sono stati ancora individuati i responsabili dell'attacco informatico. L'unica pista era nata, bizzarramente, proprio dalla canzone degli AC/DC. Quando la polizia in conferenza stampa aveva consegnato il foglio con le parole di *Thunderstruck*, un cronista si era chiesto se non fosse un karaoke. In verità, è stato proprio Brian Krebs, il giornalista che per primo ha fatto lo scoop sul leak, a prendere sul serio quella indicazione. Al punto da sospettare il coinvolgimento nell'attacco di un anonimo profilo Twitter, @deuszu.

Tutto nasce da un tweet pubblicato da questo profilo poche ore dopo l'articolo di Krebs che dava notizia dell'attacco, a luglio. Nel tweet @deuszu linkava i primi dati sottratti dagli hacker, che Krebs conosceva perché gli erano stati passati confidenzialmente proprio da Impact Team attraverso il modulo di contatto del suo sito alcune ore prima. Ma il link non era stato ancora diffuso, non c'era da nessuna parte, sostiene Krebs. Come faceva quindi @deuszu a conoscerlo a meno di non essere almeno molto vicino agli hacker? A quel punto Krebs si è scaricato cinque anni di tweet del profilo di @deuszu, notando che era a sua volta dedito all'hacking. E che un paio di attacchi contro altri siti web rivendicati da @deuszu menzionavano proprio *Thunderstruck* degli AC/DC come canzone di "accompagnamento" ai suoi messaggi. Non solo: poche ore prima che Impact Team, a luglio, venisse pubblicamente allo scoperto con la sua prima fase dell'attacco ad Ashley Madison – nota ancora Krebs – @deuszu twittava di stare configurando alcuni server. E nello "screenshot" twittato compariva una finestra di YouTube con *Thunderstruck*.

L'ipotesi di inchiodare l'hacker responsabile di uno dei colpi più clamorosi degli ultimi anni attraverso una canzone era però tanto suggestiva quanto incerta. E altri osservatori hanno da subito espresso

dubbi sulla pista individuata da Krebs. Alcuni, ad esempio, hanno fatto notare che @deuszu non sarebbe stato in assoluto il primo a twittare quelle informazioni. Inoltre, linkare pubblicamente per primo un leak non significa necessariamente esserne l'autore: al limite può voler dire avere connessioni con chi l'ha compiuto. Anche perché è interesse di chi fa un attacco non diffonderlo per primo da un account che non si vuole collegare all'hack, proprio per non attirare subito l'attenzione su di sé (a meno di non volerlo rivendicare esplicitamente, come avviene in alcuni casi). La giornalista australiana Asher Wolf ha poi ricordato come *Thunderstruck* nel 2012 – cioè quando @deuszu l'aveva usata come messaggio di accompagnamento ad alcuni suoi hack – fosse particolarmente popolare tra gli hacker per una ragione molto semplice. Pare, infatti, che fosse stata usata come sottofondo di un cyber-attacco – un altro! – al sistema nucleare iraniano.

L'episodio – che sarebbe avvenuto nel 2012, secondo un resoconto riferito da F-Secure – non c'entrerebbe con Stuxnet, il worm che, come abbiamo visto, mandò in tilt le centrifughe di Natanz tra 2009 e 2010. Sarebbe stato molto meno sofisticato e potente, ma avrebbe avuto la particolarità di riprodurre *Thunderstruck* a tutto volume nel cuore della notte attraverso alcuni dei pc infetti. Il fatto non è mai stato verificato, ma ha sicuramente solleticato la fantasia di futuri emulatori.

Un monito per tutti

Intanto la piattaforma di scappatelle non sembra aver subìto ferite irreparabili dall'aggressione e, dopo un periodo di turbolenze, ha apparentemente ripreso le sue attività come nulla fosse. Né sembrano averla scalfita alcune cause legali mosse da ex iscritti riguardo alla perdita di riservatezza e alle ripercussioni prodotte dal leak, cause che sono ancora in corso in tribunale. E non l'hanno frenata neppure alcuni reportage giornalistici che hanno evidenziato non solo lo sbilanciamento tra uomini e donne (queste ultime sarebbero state il 15 per cento, secondo il "New York Times", sebbene altre stime fossero ancora più severe), ma anche l'utilizzo di "fembot", "bot" femminili, cioè programmi automatici che simulavano identità di donne con cui attirare clienti.

A un anno dal leak, dopo un cambio di management, Avid Life Media

(che ha mutato nome in Ruby) ha tentato di scrollarsi di dosso l'infelice passato con un "rebranding" del sito, che non è più centrato sull'idea di infedeltà e vuole aprirsi a una fetta più ampia di persone. Naturalmente, l'azienda sostiene anche di aver rafforzato le proprie difese digitali attraverso un consistente lavoro di "auditing", cioè con un'analisi indipendente, fatta da società esterne, dei suoi sistemi. La Federal Trade Commission, l'agenzia federale statunitense per la protezione dei consumatori, ha però aperto un'indagine sulla società. Nel dicembre 2016 si è quindi arrivati a un accordo legale fra le parti che prevede una ammenda da 17,5 milioni di dollari. L'agenzia federale ha stigmatizzato tra le altre cose proprio l'utilizzo di bot per ingannare gli iscritti, oltre che la mancata cancellazione dei loro dati quando richiesto. Tuttavia la società dovrà versare effettivamente solo una minima parte di quella cifra, 1,66 milioni di dollari, perché sarebbe impossibilitata a pagare. E di questi soldi nulla andrà di fatto agli utenti. Forse, a lungo termine, Ashley Madison non si riprenderà mai del tutto dal colpo subito. Di sicuro, nel medio e breve termine, a pagarne le conseguenze più salate sono stati molti suoi clienti.

Perché il punto è che non c'è bisogno di essere un target per finire vittima di un attacco. Certo, se si è un ricercatore di sicurezza informatica che lavora sui malware di Stato – come abbiamo visto con Stuxnet – si potrà incorrere in un certo tipo di attenzioni dirette e *ad personam*. Ed è quasi impossibile difendersi da un attacco mirato condotto da una entità statale. Ma ciò non vuol dire che, da quella categoria in giù, non esistano dei rischi per tutti gli altri. Che non vanno considerati come una massa indifferenziata, ovviamente. Ad esempio, imprenditori e dipendenti di aziende con proprietà intellettuale di valore, militari, funzionari governativi, politici e giornalisti – soprattutto quelli che trattano temi di sicurezza nazionale – avranno comunque un profilo di rischio più elevato della media, poiché possono finire nel mirino di vari soggetti.

Tuttavia, anche l'utente più comune – proprio quello che ama dire "tanto io non ho nulla da nascondere", "tanto se il governo/criminali/spie/hacker entrano nel mio pc si annoiano" e via dicendo – può diventare vittima di un attacco. Nella maggior parte dei casi, quale danno collaterale di aggressioni che nascono con altri fini. E in alcuni episodi – che però sono sempre più frequenti, e tenderanno a crescere – vittima in quanto "utente

comune", in quanto "commodity", bene indifferenziato e interscambiabile di un sistema che lo rivenderà a pezzetti, dentro blocchi di dati passati di mano in mano. Gli utenti "normali", quelli che usano la Rete in modo "normale", medio e tendenzialmente spensierato, saranno sempre di più "utenti da cannone", prima linea di un'economia digitale – legale e criminale – basata sulla vendita di dati. Questi dati possono essere ottenuti con il consenso delle persone, quando ad esempio cliccano senza preoccuparsi su qualsiasi modulo di "Accettazione dei termini di servizio"; o possono essere esfiltrati a forza dai server di un'azienda. In questo tritacarne, in realtà, ci siamo dentro un po' tutti, ma in alcuni casi – e lo si è visto con Ashley Madison – il risultato di una fuga incontrollata di informazioni può avere conseguenze pesanti, reali e soprattutto impreviste.

"Possiamo pensare che questo leak è accaduto a dei traditori irresponsabili che si erano iscritti a un sito di incontri extraconiugali, e che quindi non ci riguarda", commenta ancora Brown. "Ma la realtà è che ha mostrato la natura del mondo ricco di dati in cui viviamo. Dove tutti siamo vittime potenziali. L'America, nelle sue radici, ha ancora una cultura puritana e questo non le ha permesso di mostrare empatia per le vittime di Ashley Madison; e di capire la natura del leak e quello che ci ha mostrato: ovvero che stiamo tutti vivendo in una gigantesca casa di vetro".

Dentro il commercio di dati

Quello di Ashely Madison non è un caso isolato. Nel giugno 2016 si è saputo che milioni di account Badoo – sito di dating fondato nel 2006, che sostiene di avere oltre 300 milioni di iscritti in centinaia di Paesi, e che almeno fino a qualche anno fa era abbastanza popolare anche in Europa, Italia *in primis* – venivano venduti nell'underground della Rete.

A comunicarlo è stato il sito Leaked Source. Si tratta di un servizio che fa da raccoglitore di leak che circolano nella Rete, andandoli a pescare tra darknet e forum russi. Il sito offre un motore di ricerca per permettere agli utenti di vedere se la propria mail compare in qualche leak, e guadagna vendendo un accesso pieno al proprio "database di database". Non è trasparente come Have I been pwned? di Troy Hunt, ad esempio non si risale facilmente ai suoi proprietari. Inoltre, pagando, permette addirittura di accedere alla password cifrata o in chiaro di qualsivoglia account, se

disponibile. Ma resta un buon indicatore dei materiali all'ingrosso che vengono scambiati in certi ambienti.

Leaked Source sosteneva di avere 127 milioni di profili Badoo – anche se l'azienda di dating ha smentito alla testata americana "Motherboard" di essere stata hackerata. Quale che fosse la loro provenienza, molti dei profili apparivano reali. E ognuno poteva contenere informazioni come indirizzo mail, nome utente, password, genere, nome e cognome, data di nascita e altri elementi.

"Non capisco perché in Italia nessuno si stia filando questa fuga di dati", mi dice in quei giorni una mia fonte che preferisce restare anonima e che aveva avuto accesso a una parte del leak. "Il mega blocco di dati è difficile se non impossibile da trovare, ma ci sono alcune 'directory' con voci consultabili. È una storia notevole anche perché una marea di utenti erano italiani. Ho già trovato miei colleghi, amici, clienti, parenti". Mi mostra alcuni esempi: profili che contengono nome, cognome, indirizzo mail, data di nascita, password cifrata (hashed) e in chiaro. Secondo Leaked Source, le password erano salvate e cifrate con metodi "non all'altezza degli attuali standard", per cui molte sarebbero state violate facilmente. Ma non è tutto. Guardando su Leaked Source i domini delle caselle di posta usate dagli iscritti, se ne trovano molti italiani: oltre 5 milioni su @hotmail.it, oltre 2 milioni su @libero.it, quasi 2 milioni su @live.it, 1,1 milione su @yahoo.it, 771mila su @alice.it, 491mila su @tiscali.it e 379mila su @virgilio.it, per un totale di oltre 12 milioni di caselle di posta. Del resto, nell'elenco delle password più usate, ne appaiono molte che alludono chiaramente a utenti tricolori: Juventus, Antonio, Napoli, amoremio, ciaociao e via dicendo.

La primavera 2016 si è distinta per molti dump di servizi importanti, cioè copie di database degli iscritti a un sito prelevate fraudolentemente non si sa bene come e quando, e improvvisamente affiorate dalle profondità della Rete. Nel maggio 2016, ad esempio, su The Real Deal, un mercato delle darknet raggiungibile solo attraverso Tor Browser, un hacker di nome Peace commerciava 117 milioni di profili LinkedIn, contenenti indirizzi mail e password. La fuga di dati era stata confermata anche da Leaked Source[17], che aggiungeva al suo motore di ricerca ben 167 milioni di profili del social network lavorativo (solo una parte conteneva anche le password). Si tratta di dati che, a quanto pare, derivavano da un attacco contro

LinkedIn avvenuto nel 2012, e che era già noto. Tuttavia, inizialmente, era stata rilasciata online solo una minima parte dei profili violati (6,5 milioni). Tutti gli altri erano rimasti dormienti da qualche parte per poi sbucare fuori di recente. Solo a quel punto si è capito che quella violazione del 2012 era molto più seria. LinkedIn ha poi mandato una mail ai suoi utenti, specificando di aver invalidato la password se l'account non l'aveva reimpostata dal 2012.

"Quando ho aperto il mio sito Have I been pwned?, volevo aiutare le persone a capire meglio la loro esposizione, in un momento in cui le violazioni e le fughe di dati stavano diventando più frequenti", mi scrive ancora Troy Hunt. E da allora ha avuto il suo bel daffare. Hunt ritiene infatti che la "tendenza di lungo termine sia certamente in crescita, specialmente quando si considerano violazioni come quelle avvenute ai danni di LinkedIn e MySpace". Numero di incidenti, quantità di dati, loro appartenenza alla sfera personale: tutti questi parametri sembrano spingere l'asticella dell'allarme verso il rosso.

In Rete esistono molti luoghi e persone specializzate nel commercio all'ingrosso e al dettaglio di profili utente. Nel 2016 alcuni di questi leak circolavano molto sul già citato The Real Deal, un eBay delle darknet. Qui – anche se le droghe restavano la categoria principale di merce/servizio in vendita, insieme alle frodi – compare anche, come sezione a sé stante, quella sui database. Addirittura ce n'è una dedicata solo ai "dati governativi". Uno dei venditori più attivi, con buoni feedback dagli altri utenti, si chiama BestBuy. Tra le altre cose, nel luglio 2016, vendeva proprio il database di profili LinkedIn: 117 milioni di mail e password per 1,6 bitcoin (circa 963 euro mentre scrivo). È lo stesso database venduto da Peace (il primo hacker che lo aveva messo in vendita), specifica l'annuncio, "ma la sua inserzione non c'è più".

BestBuy vende anche il database del World-Check, una sorta di archivio di sospetti terroristi compilato dalla società Thomson Reuters e usato – non senza polemiche sui suoi criteri di compilazione – da una cinquantina di banche in tutto il mondo, oltre che da trecento agenzie di intelligence. Poche settimane prima era emerso che i suoi dati – 2,2 milioni di voci – erano presenti in Rete, in qualche modo "leakati". BestBuy, inoltre, vende 40mila mail, nomi utente, password in chiaro (ottime per il riuso, specifica l'annuncio) e altre informazioni su clienti di farmacie online. "Freschi

freschi, rubati da siti hackerati", recita la descrizione.

Contatto BestBuy attraverso il sistema di messaggistica del sito e chiedo alcuni chiarimenti. "I dati delle farmacie online sono buoni per fare spam, sono presi da vari siti", mi scrive. Invece per quanto riguarda i profili LinkedIn, quando gli chiedo a che servirebbero dal momento che la piattaforma ha già cambiato di default tutte le password, spiega che a questo punto sono buoni per il riuso delle stesse. Significa che un hacker prova a usarle su altri profili delle vittime, contando sul fatto che molte persone tendono a riutilizzare le stesse parole chiave per siti diversi. BestBuy mi dice di ottenere questi database in vari modi e di guadagnarci abbastanza.

Su un altro sito, AlphaBay, uno dei più importanti mercati neri del Deep Web, un altro venditore, AccountShop, nel giugno 2016 aveva messo in vendita account da oltre 200 siti. Tra questi spiccavano anche username e password di utenti Trenitalia, venduti a 8 dollari l'uno (ben più cari della media). Poi c'erano profili Airbnb, a 4,30 dollari l'uno. EasyJet a 2,90 dollari. Groupon tra 1 e 1,20 dollari. LinkedIn a 2,90 dollari. Zalando a 5 dollari. E molti altri ancora. Non ho potuto verificare se gli account in vendita fossero autentici e funzionanti, ma la reputazione del "negoziante" e i feedback dei suoi clienti erano abbastanza buoni. "Sono un rivenditore, conosco un sito che vende questi account a prezzi più bassi, li compro lì e li rivendo qua", mi scrive AccountShop attraverso il sistema di messaggistica di AlphaBay. "Vendo circa 500 account al mese. In media guadagno tra i 30 e i 90 dollari al giorno, ma a volte ho delle vendite in massa e faccio di più. Dei profili Trenitalia non so nulla di specifico".

Un altro venditore del sito, Bestworks, con 456 recensioni positive, smerciava invece un dump massivo di oltre 10mila account internazionali hackerati, da Amazon a Dropbox e Instagram. Mentre su un mercato minore, T•chka, che ha peraltro un codice di condotta curioso[18], un hacker aveva messo in vendita il database di un popolare sito francese di modelle, anche se i dati erano limitati a nomi e indirizzi mail.

"Il commercio di dati rubati è profittevole quando i costi di chi lo compie sono così bassi. Nel senso che lo sforzo di hackerare i dati è spesso minimo o è frutto di accordi e scambi con altri hacker, e le informazioni divengono una merce di scambio", mi spiega ancora Hunt, specificando che la modalità di attacco più diffusa per trafugare questi dati resta ancora –

insieme alla violazione di password deboli e all'ingegneria sociale – la Sql Injection. "Gli account prelevati sono poi usati per compromettere altri servizi o per contribuire a furti d'identità. Quando hai decine o forse centinaia di milioni di voci ('records'), il costo per identità è quasi inesistente".

Una delle mercanzie destinate purtroppo a riversarsi sempre più spesso su queste bancarelle virtuali sono le informazioni di natura sanitaria, che come si può immaginare sono particolarmente sensibili. Tornando al mercato The Real Deal, nel luglio 2016 un hacker noto come The Dark Overlord ("chiamatemi il Dottore, gente", era il suo motto) vendeva i dati di 689mila pazienti americani divisi in più database appartenenti a diverse organizzazioni mediche. I prezzi – per ottenere una unica copia, così prometteva l'hacker – andavano da 151 bitcoin (circa 100mila dollari) a 607 bitcoin (395mila dollari). Difficile immaginare degli acquirenti per prezzi così elevati, ma è senz'altro un indicatore del maggior valore di questo genere di informazioni. Le istituzioni colpite erano la Midwest Orthopedic Clinic del Missouri, con 48mila profili di pazienti, inclusi username e password in chiaro; una seconda organizzazione di questo tipo, non specificata, in uno Stato del Midwest, per un totale di 210mila profili; e una terza dello Stato della Georgia, con 397mila profili. Alcuni dei dati in questione erano stati verificati come autentici da vari ricercatori. Cosa si può fare con informazioni del genere? "In generale furti d'identità nel significato più ampio", commentava lo stesso The Dark Overlord su un forum.

"Il furto di dati medici e di assicurazioni perpetrato da The Dark Overlord è l'ennesimo di una serie di violazioni e di cyber-attacchi che stanno colpendo organizzazioni sanitarie", hanno scritto al riguardo gli analisti di Trend Micro, che proseguono elencando – solo negli Stati Uniti – le vittime: cliniche, ospedali e strutture sanitarie in Arkansas, California, Massachusetts, Nebraska, New Mexico, Tennessee e Texas. Un'epidemia.

"La salute rimane un target centrale di 'ransomware' [di cui parleremo tra poco], furto di informazioni e attacchi di phishing mirati". Insomma, i cyber-criminali – ammonisce Trend Micro – considerano questa industria una fonte redditizia di informazioni personali e d'identità, che spesso si accompagnano a dati finanziari, e tutto ciò è facilmente monetizzabile nei mercati underground. Informazioni che possono essere usate per frodi,

appropriazione d'identità e di proprietà intellettuale, spionaggio, ricatto, estorsione. In prospettiva, questa rischia di diventare una delle praterie più ricche dove andrà a pascolare l'economia cyber-criminale. Specie se dovessero esaurirsi le risorse che ora stanno alimentando – come vedremo nel prossimo capitolo – una delle più sfacciate industrie di estorsione di massa.

[15] Si ricordi il caso del Celebgate, quando nel 2014 le foto private di un centinaio di star e vip americani finirono online. Erano state trafugate dai rispettivi account iCloud e Gmail da un hacker che aveva ottenuto le credenziali delle vittime inviando loro mail di phishing.

[16] https://www.troyhunt.com/heres-what-ashley-madison-members-have/.

[17] https://www.leakedsource.com/blog/linkedin.

[18] I codici di condotta non sono inusuali nei mercati del Deep Web – ne aveva uno anche Silk Road, il primo mercato di droghe nelle darknet –, ma questo è molto definito: il sito non accetta sostanze sintetiche poco note, armi, veleni ed esplosivi, pornografia, contenuti relativi ad estremismo, nazionalismo e antisemitismo o altre forme di discriminazione.

4.
La fabbrica delle estorsioni

Incontro col venditore

“Dimmi, sei qua per il servizio?”, mi chiede il venditore appena lo contatto attraverso una chat cifrata. Il suo indirizzo lo avevo recuperato dopo un po’ di lavoro di scavo su forum russi e avevo provato a cercarlo al volo. Era online e mi aveva subito risposto. “Sì, cioè volevo sapere, non ho capito bene: vendi kit di ransomware?”. “300 dollari il prezzo completo”, mi risponde, per poi partire con una serie di messaggi velocissimi e in un inglese pirotecnico che cominciano a snocciolarsi sul mio monitor. “Avrai accesso al pannello di comando e controllo per configurarti il malware. Aspetta un minuto che ti do l’indirizzo bitcoin dove girarmi i soldi. Tieni ecco qua: sono 0,7198904 bitcoin [circa 300 dollari all’epoca]”. Provo a interromperlo. “Ma il software qual è, Cryptolocker?”. “Fammi sapere quando hai depositato i soldi, così appena arriva la transazione ti configuro il profilo per l’accesso. Sì, è Cryptolocker”. “Ma è localizzato in diverse lingue?”. “Sì, ti faccio configurazione e lingua come vuoi. Fammi sapere quando arrivano i soldi”. “No, aspetta, volevo solo avere delle informazioni”. Il venditore a questo punto inizia a imprecare. “*Oh man*. Cosa vuoi, un pasto gratis? Qui le consultazioni si pagano, tutti pagano, ho incassato 98 bitcoin [65mila dollari] finora. E tu arrivi e pretendi di avere informazioni? Ma sei normale? Ho investito la mia energia già per 30 minuti dietro a te!”.

Erano forse cinque o dieci minuti in verità, e provo stupidamente a obiettarlo nella vana speranza di sedarlo. “Cosa vuoi, la pappa gratis? Vai a imparare come si programma e fatti il tuo prodotto!”. Insisto, provo a cambiare argomento con un: “Scusa, ma da quanto tempo vendi ransomware?”, e il risultato è che lui passa al TUTTO MAIUSCOLO. “DEVI

PAGARE PRIMA DI TUTTO, HAI CAPITO?". Seguono imprecazioni. "MA CHI SEI, UN DETECTIVE? UN BRIAN KREBS? UN PROVOCATORE?". Brian Krebs è il giornalista tech investigativo che abbiamo già incontrato nel capitolo precedente. È molto famoso da queste parti perché ha infiltrato per anni i forum di cyber-criminali russi, ricostruendo molte delle loro attività, soprattutto il modo in cui orchestravano massicce campagne di spam e frodi. Per ringraziarlo dell'attenzione, i suoi "amici" online gliene hanno fatte di tutti i colori: ad esempio, gli hanno spedito delle partite di droga a casa sua per metterlo nei guai. E una volta, attraverso una finta richiesta di aiuto che simulava di arrivare dalla sua utenza telefonica, gli hanno fatto piombare in casa una unità speciale della polizia armata di tutto punto.

Ad ogni modo, di fronte all'agitazione del tipo, provo a battere in ritirata. "Ok, lascia perdere, scusa se ti ho disturbato". Ma quello non demorde, è proprio infuriato e parte con una filippica. "Senti, Mr [segue il mio nickname volutamente storpiato] dei miei stivali, il mio tempo è denaro! Devo pagare l'affitto dell''hosting', gli 'script', i malware. SE NON PAGHI IMPARA DA SOLO!".

L'esplosione dei ransomware, "i malware del ricatto"

Così è terminata una delle mie conversazioni online con un venditore di cyber-estorsioni. Per fortuna non sono state tutte così accalorate. Ma per capire di cosa si tratta bisogna fare un passo indietro. Il tipo contattato in chat vende, per 300 dollari da pagare con la moneta elettronica bitcoin, l'affiliazione al suo sistema di ransomware. Con questo nome (da "ransom", "riscatto", e software) si indicano dei software malevoli che, dopo aver infettato un pc, limitano l'accesso ad alcune sue parti, nel caso specifico criptandone i file e chiedendo un riscatto al suo proprietario per permettergli di decifrarli.

Ci sono tanti tipi di ransomware, ma quelli più insidiosi usano sistemi di cifratura molto complessi che rendono impossibile recuperare i file senza avere la chiave. "Inoltre, alcuni eliminano ogni traccia della chiave dal sistema e arrivano anche a mantenerne una copia soltanto sui loro server, criptata, così da evitare di perderle o diffonderle a seguito di un attacco (permettendo alle vittime di decifrare i propri documenti senza pagare il riscatto)", mi spiega Paolo Dal Checco, dello studio di informatica forense

DiFoB di Torino, una delle persone che in Italia hanno monitorato di più il fenomeno al punto da aver aperto anche un sito apposito, Ransomware.it.

Questo li rende un'arma perfetta per ricatti di massa: se non paghi, non riavrai i tuoi documenti, magari materiali importanti e urgenti o le foto di una vita. Tutto quello che devono fare gli estorsori è scrivere dei malware di questo tipo, procurarsi delle liste di utenti a cui inviarli e – quando le infezioni vanno a segno – creare degli indirizzi bitcoin unici per ogni utente su cui indirizzare le vittime; una volta che queste pagano, viene inviata loro la chiave di decriptazione insieme a un software ("decryptor").

La filiera delle cyber-estorsioni

Cosa serve tecnicamente per mettere in piedi questa fabbrichetta di estorsioni multiple? Il malware, ovvero i file eseguibili che infettano il pc procedendo poi con la cifratura dei file: chiamiamoli l'arma vera e propria. Un server dove piazzare un centro di comando e controllo (C&C) con cui mantenere la comunicazione con i computer infettati: chiamiamola la stanza dei bottoni. Un sistema con cui veicolare i malware verso i destinatari, e che in genere si compone di finte mail con allegati che procedono all'infezione una volta aperti o con dei link che rimandano a siti che ti infettano attraverso ulteriori link o direttamente per la vulnerabilità del browser: chiamiamolo il mezzo di lancio dell'arma o, meglio ancora, la rete distributiva. Infine, serve aprire dei portafogli bitcoin con cui generare indirizzi preferibilmente unici da fornire a ogni vittima per i pagamenti: chiamiamolo il sistema di riscossione.

Ora, in questa impresa criminale così segmentata, è chiaro che la distribuzione può essere data in franchising, esattamente come puoi aprirti un negozio di fast food per conto di un noto brand che ti farà arrivare i suoi hamburger. Nel caso del venditore citato all'inizio, se lo avessi pagato, lui mi avrebbe inviato un file eseguibile (il malware) che avrei dovuto usare per infettare le mie vittime, nonché l'accesso a un pannello con cui monitorare le infezioni, i pagamenti e accedere alla mia parte di guadagni. Io avrei dovuto soltanto confezionare una mail fasulla credibile – magari una finta bolletta proveniente da qualche nota utility dell'energia o da una compagnia telefonica – e procurarmi una lista di destinatari. Non avrei

dovuto occuparmi di scrivere il malware, né di configurare un server per controllare i computer infettati da remoto. Il venditore, da parte sua, moltiplica i guadagni affittandomi la sua infrastruttura. O, anche senza noleggiare nulla, ritagliandosi direttamente una percentuale su ognuna delle mie vittime.

Il centro di comando e controllo ha due funzioni, mi spiega Dal Checco. La prima è quella di ricevere le chiavi con cui sono stati cifrati i file di ogni computer colpito, catalogandole per pc, così il gestore sa quanti ne ha infettati e ha le chiavi di sblocco per ognuno di loro. La seconda funzione è quella di gestire il pagamento del riscatto, spesso in modo automatizzato. Infatti il centro di comando e controllo si interfaccia con i siti delle darknet dove le vittime devono connettersi per scoprire a quale indirizzo bitcoin versare il riscatto e poi scaricare il decryptor, ovvero il software di decifrazione con la chiave. A quel punto la vittima avvia lo strumento, carica il file con la chiave e il programma comincia a decriptare tutti i file criptati.

"Spesso questi software non sono scritti bene, non decifrano tutto o si piantano. In alcuni è persino stato trovato altro malware al loro interno", aggiunge Dal Checco. Naturalmente non tutti i ransomware usano questi sistemi. "Alcuni sono più artigianali e i delinquenti, invece di lasciare il messaggio con la richiesta di riscatto, attaccano al nome del file l'indirizzo mail su cui la vittima li può contattare per sapere come e dove pagare, per poi ricevere – via mail – il decryptor". Ci sono stati anche estorsori che comunicavano con le vittime attraverso servizi come One Time Secret, che permettono di inviare messaggi che si autodistruggono una volta letti, così da non lasciare tracce.

I programmi di affiliazione

Questa architettura – insieme all'efficacia dei ransomware nell'infettare i dispositivi – ha moltiplicato i programmi di affiliazione. Ne esistono anche di automatizzati. Uno dei primi di questo tipo, di nome Tox, era stato scovato dai ricercatori di McAfee. Funzionava così. Si andava su un sito ospitato nelle darknet a cui ci si poteva "iscrivere" gratuitamente. Poi si scaricava il virus da inviare alle proprie vittime designate. Queste avrebbero pagato i riscatti a chi gestiva Tox, che poi avrebbe versato i soldi

sull'indirizzo bitcoin inserito dall'affiliato. Mentre i gestori si trattenevano una quota del 30 per cento.

Tox non era l'unico programma del genere. Nella primavera del 2016 ne ho provato uno simile, sempre ospitato sulle darknet. Ho messo l'indirizzo bitcoin dove volevo che fosse pagata la mia parte degli incassi; ho configurato il malware in base alle mie preferenze (scegliendo quanto chiedere di riscatto alle vittime e quanto tempo concedere loro per pagare); e ho scaricato il malware. A quel punto dovevo solo diffonderlo. Cosa che ho fatto, ma limitandomi a girare il virus a due esperti di sicurezza informatica. "Non è molto sofisticato, ma fa il suo lavoro. Il fatto è che questi malware non hanno bisogno di essere tecnicamente complessi, anzi, più sono semplici e più sono funzionali, perché sfuggono agli antivirus. La parte più evoluta sta semmai nella diffusione del malware", mi ha spiegato Alberto Pelliccione, che abbiamo già incontrato in precedenza. Fondatore della società ReaQta, che offre alle aziende soluzioni avanzate di difesa basate sull'intelligenza artificiale, dal 2015 si è trovato suo malgrado, come molti altri del settore, a dover gestire anche un'epidemia di estorsioni. Nonché a inseguire le tracce di alcuni dei loro burattinai, come vedremo tra poco.

Ad ogni modo – mi spiega – la forza dei ransomware è che sono semplici da scrivere e se ne possono generare in continuazione e in grandi quantità, usando poi delle tecniche per offuscarli e renderli invisibili. Essendo programmi nuovi, spesso gli antivirus non li riconoscono. A quel punto la sfida è solo rendere minimamente credibile la mail (il vettore di attacco più usato) che li veicola.

"La ragione per cui stanno tutti balzando sul carro è molto semplice: sono soldi facili", mi scrive in chat un altro venditore di kit di cyber-estorsioni. Rispetto al primo intervistato è molto più tranquillo, e dice che posso pure citare il suo "nickname", il suo pseudonimo online, Tartarus. L'ho incrociato a partire da forum russi come *Exploit.in*, sebbene non credo sia di quelle regioni. "I programmi di affiliazione sono comodi, perché liberano gli affiliati dai costi di gestione dell'infrastruttura di controllo del malware e dei pagamenti". Lui lo sa bene, visto che offre a sua volta uno di questi ransomware in franchising. Paghi subito 100 dollari in bitcoin – mi spiega – e lui ti dà un file eseguibile, il virus, che si è scritto da solo, da distribuire sui computer delle vittime, nonché l'accesso a un pannello di

controllo per monitorare le infezioni. Di tutti i riscatti incassati si prende il 15 per cento. Dice di avere 300-400 clienti.

"Sono soldi facili", mi ribadisce un altro, contattato online, che fa parte del team Cfud. Si tratta di un gruppetto che circola ancora sui forum russi ma che si è aperto anche un sito nelle darknet, una sorta di mercato per hacker dove scambiarsi servizi e da cui loro guadagneranno con una percentuale sulle vendite. Quando gli parlo il loro mercato è online da poco, ma ha già due venditori di ransomware. I riscatti vanno da 250 a 500 dollari, quindi basta mettere a segno una parte delle infezioni e delle successive richieste di pagamento, mi spiega. Ma quanto costa imbastire una campagna di questo tipo?, gli chiedo. "Occorre avere un server, più alcuni domini (siti web), più dei virus: i server costano tra i 25 e i 50 dollari; i domini tra 1 e 10 dollari; i virus ('payload') fra i 100 e i 1000 dollari per un migliaio di installazioni". Fatti due conti, le spese iniziali si ammortizzano in fretta. Va anche detto, aggiunge il membro del team Cfud, che in Rete ci sono tanti annunci del genere, ma la qualità dei prodotti (dei virus) è spesso bassa.

Nascita e sviluppo di un modello di business cyber-criminale

I ransomware, intesi come software malevoli che limitano l'accesso di un utente al suo computer o ai suoi contenuti, sono piuttosto antichi. Il primo del genere risale addirittura al 1989, l'anno della caduta del Muro di Berlino, per intenderci. Si trasmetteva via floppy disk e arrivava nella cassetta della posta, quella fisica, delle lettere, che sta fuori dalla porta di casa o dal portone. Simulava di essere un programma informativo sull'Aids, che era esploso solo pochi anni prima negli Stati Uniti. Attribuiti a un'azienda inventata, la PC Cyborg Corporation, i floppy disk (ben 20mila) contenevano realmente un programma che sottoponeva gli utenti a una sorta di quiz interattivo per determinare il loro livello di rischio di contrarre l'Hiv. Tuttavia, trasmettevano anche un trojan, un virus poi ribattezzato per l'appunto Aids, che cifrava i file delle sue vittime dopo un certo numero di avvii del computer. Una volta entrato in azione, il malware indicava agli utenti di stampare la richiesta di riscatto, mascherata come una sorta di licenza da pagare per il programma: 189 dollari da girare su una anonima cassetta postale panamense, per ottenere di fatto la chiave

di decriptazione.

La storia del trojan Aids è particolarmente bizzarra perché a realizzare il malware e a mandarlo in giro fu un biologo con un dottorato ad Harvard, Joseph L. Popp, che era effettivamente coinvolto, anche se in modo marginale, in alcuni progetti sulla Sindrome da immunodeficienza acquisita. Il suo movente, però, non è mai stato chiarito del tutto. Voleva vendicarsi per un presunto sgarbo subìto dalla comunità scientifica? Raccogliere davvero dei soldi per la lotta all'Aids come una specie di cripto-Robin Hood? Oppure era un folle, ma abbastanza meticoloso e ben organizzato da imbastire uno schema truffaldino per l'epoca grandioso? Difficile capirlo. Il fatto è che, dopo essere stato arrestato da Scotland Yard, al processo è stato dichiarato infermo di mente.

"L'innovazione maligna del dottor Popp – ovvero trasformare il software in un veicolo per ricatti internazionali – era soprattutto concettuale", scrive la scrittrice Alina Simone, che si è appassionata al tema dopo aver subìto in prima persona l'effetto dei ransomware. "La forma di crittografia che aveva usato per sequestrare gli "hard disk" delle vittime, nota come crittografia simmetrica, era facilmente reversibile". Già, quel tipo di crittografia lo era ancora, ma non quella asimmetrica, basata su due chiavi, una pubblica e una privata, diffusasi successivamente. Inoltre, quella di Popp era una iniziativa isolata, anomala, forse opera di un pazzo, in ogni caso riconducibile a un solo individuo.

Lo scenario inizia a cambiare a metà degli anni Duemila, quando cominciano a diffondersi i primi "blocker", specie in Russia. I blocker sono malware che impediscono agli utenti di usare il pc bloccandone lo schermo o la tastiera. In alcuni casi fingono di essere un messaggio delle forze dell'ordine, una sorta di multa per aver fatto qualcosa di illegale, per aver piratato dei film o aver guardato contenuti pedopornografici. La presunta ammenda andava dai 50 ai 200 dollari, da pagare con carta di credito o attraverso l'invio di messaggi a servizi sms premium. Sebbene anche in questo caso il blocco fosse di fatto reversibile, l'invio di massa sembrava funzionare: una parte delle vittime pagava. L'epidemia fu tale che furono avviate varie inchieste, gli operatori telefonici dovettero rivedere le regole con cui assegnavano numeri premium (su cui ricevere pagamenti via sms), e infine nel 2010 ci fu una maxi-retata a Mosca.

Ma nei forum underground esistevano già kit fai-da-te per crearsi un

blocker: insomma, non bisognava essere dei programmatori di alto livello per partecipare al business. Perché di questo si trattava, ormai: la commercializzazione del malware e la definizione di schemi di distribuzione standardizzati erano ormai decollati.

In questo scenario, il salto di qualità avviene nel 2013, con l'emersione di una nuova varietà di ransomware che sfrutta la crittografia asimmetrica di cui si diceva sopra e algoritmi di cifratura molto complessi. Significa che, nella maggior parte dei casi, la loro azione non è più reversibile senza la chiave, quella privata, fornita dagli stessi criminali. Questo genere di malware viene spesso definito "crypto-ransomware" o anche solo "cryptor", dove il termine "crypto" allude proprio all'uso della cifratura – specie quella cosiddetta asimmetrica – per rendere inutilizzabili i file dei computer infettati.

Il primo della categoria a diffondersi ampiamente, a partire dal 2013, è stato ribattezzato CryptoLocker. Ne sono seguiti altri, che hanno introdotto continue variazioni. Tra i sistemi di pagamento inizia a diffondersi l'uso di bitcoin, la moneta elettronica che, se usata con vari accorgimenti, riesce a offrire un buon livello di anonimato. Nel 2014 la società Trend Micro individua due varianti di un nuovo malware di questo tipo, chiamato BitCrypt, che presenta una richiesta di riscatto in dieci lingue diverse da pagarsi tassativamente in bitcoin.

I primi cryptor rilasciati dai criminali erano però ancora rozzi. Spesso i loro effetti erano reversibili perché magari la chiave di decriptazione era nascosta nello stesso apparecchio infettato e si trattava solo di trovarla. Oppure gli esperti di sicurezza riuscivano a fare "reverse engineering" (ingegneria inversa) del malware, lo analizzavano e ne ricostruivano il funzionamento al punto di trovare il modo di decriptare i dati.

Ma col tempo gli strumenti usati dagli attaccanti si sono affinati. Oggi la maggioranza di questo tipo di ransomware genera una chiave unica per la decriptazione per ogni singolo apparecchio infettato, per cui anche se si ottiene accesso a una chiave per un determinato computer non la si potrà usare per liberare anche gli altri. Inoltre, gli schemi di cifratura sono sempre più sofisticati. In alcuni casi incapsulano uno dentro l'altro algoritmi diversi come Aes e Rsa: il primo è particolarmente veloce nel cifrare i dati; il secondo, più potente, viene usato per blindare a sua volta la chiave Aes. Inoltre, alcuni di questi gruppi usano con perizia una

combinazione di tecnologie per anonimizzarsi, abusando sia della rete Tor sia di bitcoin.

Variazioni e innovazioni sul tema

Una volta infettato un apparecchio e resi illeggibili i suoi file, il cryptor mostra un messaggio o un box in cui si spiega come pagare il riscatto, che va in media dai 300 ai 500 dollari. In genere c'è anche un limite di tempo entro cui pagare (tra le 48 e le 72 ore), sforato il quale il rischio è che il prezzo per ottenere la chiave aumenti. O che addirittura sia cancellata la stessa, rendendo i file irrecuperabili. Quali garanzie ci sono di ottenere la chiave se si accetta di pagare? Nessuna. È vero che in molti casi i criminali vogliono effettivamente far decifrare i file in ostaggio, anche per dare continuità e credibilità al loro stesso business (se non lo facessero, dopo poco tempo nessuno più pagherebbe). Ma in alcuni casi, più mordi-e-fuggi, hanno intascato i soldi e se ne sono infischiati. In altri, non infrequenti, va storto il processo di decriptazione perché alcuni di questi software contengono dei bachi che creano malfunzionamenti. O perché intervengono altre variabili impreviste nella gestione del business.

Le autorità si raccomandano ovviamente di non versare i soldi, e lo stesso consigliano gli esperti di cyber-sicurezza. Tuttavia, come ha commentato Mikko Hypponen di F-Secure in un incontro cui ho assistito a Helsinki: "Non consigliamo di pagare il riscatto. Tuttavia capiamo perché alcune persone decidano di farlo. Pensiamo al caso di un utente che abbia perso tutte le sue foto". Va però ricordato, prosegue Hypponen, che pagare alimenta il problema più generale. Nel 2012, secondo la società Symantec, la percentuale pagante degli utenti infettati era il 3 per cento. Nel 2014 il dato si è impennato al 41 per cento, secondo i dati dell'Università del Kent. Un'altra stima di Trend Micro lo attestava al 30 per cento. Sta di fatto che un simile incremento è dovuto proprio all'uso di sistemi di cifratura più sofisticati.

Si è arrivati così al biennio 2015-16, in cui la diffusione dei ransomware è esplosa. Il numero totale di utenti che hanno incrociato un tale malware tra l'aprile 2015 e il marzo 2016 è cresciuto del 17 per cento rispetto all'anno precedente, passando da 1.967.000 a 2.315.000, secondo un report di Kaspersky. E ancora: nell'aprile 2016, il 54 per cento delle infezioni di

questo genere era prodotta da crypto-ransomware. Le famiglie più diffuse in questo specifico genere erano TeslaCrypt, CTB-Locker, Locky, Petya, Jigsaw, Scatter e Cryakl. I Paesi più colpiti variano a seconda delle analisi, e comprendono India, Russia, Kazakistan, Stati Uniti, Germania e Gran Bretagna. Quale che sia il report di riferimento, l'Italia è sempre stata nelle prime posizioni di questa infausta classifica. E ad accorgersene all'improvviso sono stati gli esperti di sicurezza.

"Ogni settimana ho un cliente che arriva per questo", mi ha raccontato Stefano Fratepietro, fondatore dell'azienda di sicurezza informatica Tesla Consulting di Bologna. L'impennata è iniziata alla metà del 2015, al punto che la sua società ha dovuto mettere in piedi una unità dedicata appositamente ai ransomware e alle risposte d'emergenza da dare alle organizzazioni colpite. "Una di queste, che forniva buste paga a numerosi enti, si è trovata tutti i file e i documenti cifrati intorno al 20 del mese, pochi giorni prima di dover distribuire i cedolini", spiega Fratepietro. Panico, chiamata al consulente, straordinari notturni. Ma alla fine la scelta dell'azienda è stata quella di pagare.

I ransomware non risparmiano nessuno. Hanno iniziato a mietere vittime tra utenti comuni, poi aziende, quindi ospedali ed enti pubblici. A volte colpiscono senza distinzioni, altre volte prendono di mira dei target precisi. In Italia i virus arrivano soprattutto attraverso mail che fingono di essere bollette Telecom, Enel o ricevute di corrieri che dicono di non essere riusciti a consegnare un pacco, per cui l'utente deve scaricarsi il modulo per richiedere la consegna. La finta bolletta Enel è molto diffusa, mi hanno detto vari consulenti. È perfino citata in un rapporto globale sul tema realizzato dalla società Nya International, che racconta come vengano colpiti anche i servizi postali nei vari Paesi. Una campagna che ha attaccato la Royal Mail, cioè gli utenti delle poste inglesi, con mail finte, è arrivata a ben 10 milioni di britannici e ha prodotto 250mila vittime.

Il responsabile Ict di una importante università italiana mi spiega, sotto anonimato, di aver visto molti ransomware. "Le prime mail che arrivavano erano molto rozze e fatte con traduttore automatico; poi è stato evidente che è entrato in gioco qualche italiano e sono migliorate, anche se c'è sempre qualcosa che non torna". L'imperfezione non impedisce però la truffa. Gli attaccanti contano sulla imperizia, fretta e disattenzione degli utenti, e sul fatto che nelle aziende e nelle organizzazioni alcuni account

mail possono essere gestiti da più persone, il che li rende più vulnerabili.

È probabile che le mail inviate a utenti italiani siano scritte col traduttore automatico o chiedendo aiuto a dei connazionali, ma che vengano gestite comunque da altri, mi aveva detto Tartarus, uno dei venditori di ransomware. "Secondo me invece qualche italiano inizia ad esserci", commenta dal suo canto Paolo Dal Checco.

Anche Fratepietro è convinto che vi sia un pezzetto di business italiano. "In un caso abbiamo visto mail con finte bollette Hera", spiega, riferendosi alla multiutility che opera in Centro Italia. E racconta un episodio ancor più inquietante. "Dei criminali sono entrati nella rete di un'impresa, una grande azienda a conduzione famigliare. Sono riusciti ad accedere alle applicazioni usate dal dipendente amministrativo, e da lì potevano fare operazioni direttamente sul software gestionale dell'azienda e sul suo 'internet banking'". A quel punto gli attaccanti provano a dirottare i flussi del loro target, dirigendo i pagamenti bancari dell'azienda verso propri conti. È un tipico caso di frode mirata alle imprese, che punta a sequestrare i suoi versamenti senza che questa nemmeno se ne accorga. Solo che l'operazione non va in porto, la banca fiuta qualcosa di anomalo e li blocca. "A quel punto, probabilmente irritati, decidono di far detonare la bomba", spiega Fratepietro. Ovvero cifrano i file e gli asset più importanti, bloccando il software gestionale – usato per buste paga e pagamenti dei fornitori – oltre a listini, verbali, documenti, e congelando di fatto le attività dell'azienda. Insomma, hanno cifrato tutto ma – e questo è il dato inquietante – senza chiedere alcun riscatto. "Per vendetta, per sfregio, con una modalità mafiosa. E gli autori sono sicuramente italiani, perché ho trovato pezzi di codice con commenti in italiano".

Alcune delle finte mail che veicolano i ransomware sono scritte abbastanza bene; molte altre, però, presentano incongruità talmente evidenti, a partire dall'italiano balbettante, che ci si chiede come sia possibile che qualcuno possa esserne ingannato. "Il problema è che molte persone non sono abituate a considerare in modo critico quello che arriva loro via mail o sul computer, mentre non aprirebbero mai la porta ad uno sconosciuto", commenta ancora il responsabile Ict dell'università.

Il virus arriva attraverso gli allegati delle mail, spesso un file Zip o Rar mascherato da documento Word o file Pdf. Quando lo si apre, si esegue il programma e si rimane infettati. Può anche essere un vero documento

Word/Excel che chiede di abilitare le macro, e in quel modo trasmette l'infezione ("non schiacciate mai il tasto *Abilita i contenuti*", ha ripetuto in più occasioni Mikko Hypponen parlando proprio di ransomware). Oppure nella mail non c'è alcun allegato, solo un link che punta a un sito esterno, che finge di essere quello di un'azienda, di una compagnia telefonica o dell'energia e via dicendo. Da lì ci fa scaricare un documento, ad esempio la bolletta.

L'utente non si accorge di nulla. A volte viene generato un falso errore, come se il documento fosse corrotto. Ma intanto il programma si installa e inizia a criptare i file. Parte dal disco locale e prosegue seguendo le periferiche collegate – chiavette Usb, dischi esterni. Il malware lavora in "background", in modo discreto, e quando ha finito compare l'avviso con la richiesta di riscatto.

Prevenire è meglio di curare

La miglior forma di prevenzione è tenere copie aggiornate dei dati. "Noi in genere abbiamo i backup, per cui ci limitiamo a cancellare la macchina infetta e recuperiamo i dati. Ovviamente si possono perdere quelli dell'ultimo giorno di lavoro", commenta ancora il responsabile dell'Ict dell'università. Ma molte piccole e medie aziende, che magari sono cresciute in fretta senza preoccuparsi troppo della parte Information Technology e tanto meno della security, possono trovarsi con backup non aggiornati o incompleti. E quindi con il rischio di essere ricattabili. "Peraltro anche ripulire i pc, ripristinare le postazioni e recuperare i backup è un carico di lavoro aggiuntivo che produce un danno economico", aggiunge l'esperto dell'ateneo.

Prima abbiamo visto come il fenomeno, nelle sue dimensioni più organizzate, sia partito dalla Russia. Oggi quello Stato e le aree limitrofe restano ancora l'epicentro dell'ondata di cyber-estorsioni. "Ci sono diverse gang criminali, la maggior parte sono dell'Europa dell'Est, alcune hanno migliori canali di distribuzione di altre", mi ha spiegato Jérôme Segura, ricercatore di sicurezza dell'azienda californiana Malwarebytes. "Ma abbiamo visto anche molti criminali saltare sul carro dei ransomware perché è un modo molto efficace di raccogliere soldi senza intermediari". Molti soldi, e facili, come dicevamo all'inizio. Sebbene sia arduo

quantificare il fenomeno, ci sono stime parziali che fanno scorgere l'entità del mercato. Ad esempio, nel 2013 CryptoLocker avrebbe prodotto 30 milioni di dollari di ricavi in soli 100 giorni, secondo i calcoli di Dell SecureWorks.

Geografia criminale

Individuare questi gruppi criminali, da parte delle forze dell'ordine dei Paesi colpiti, soprattutto nel Nord America e nell'Europa occidentale, non è facile. "L'origine di queste campagne è in Russia e nell'Est Europa – mi conferma anche Santiago Pontiroli, ricercatore di punta della società di sicurezza Kaspersky – e rimane molto difficile individuarne gli autori anche per complicazioni o cavilli legali". Peraltro molte di queste gang stanno attente a non dare troppo fastidio ai Paesi in cui si trovano. "Le tecnologie vendute sui siti e mercati russi tendono a non affliggere utenti residenti negli Stati vicini a quei mercati", spiega Luca Allodi, ricercatore dell'Università di Trento che ha studiato quel tipo di ecosistemi. "Ad esempio i malware russi tendono a non colpire Stati dell'ex blocco sovietico. Prima di installarsi profilano il sistema attaccato: controllano per esempio se la tastiera ha un layout russo".

Il ransomware Cerber, nato proprio nell'underground dell'Est Europa, fa esattamente questo, specifica ancora Segura: "Verifica il Paese in cui si trova la vittima e batte in ritirata se si tratta di Russia, Ucraina o altri Stati dell'ex blocco sovietico". Cerber rappresenta bene anche la capacità di innovazione di questo tipo di software, perché ha introdotto una caratteristica aggiuntiva particolare: parla direttamente alle sue vittime. Attraverso una funzione "da testo a voce" ("text-to-speech") trasmette via audio le richieste dei cyber-criminali.

Uno dei settori dove si è sviluppata più competizione è stato proprio quello della customer care, la cura del cliente-vittima. Siti web in varie lingue; guide e Faq su cosa fare e come pagare; un servizio clienti che risponde a domande e richieste in modo efficiente; in alcuni casi addirittura una chat con un operatore. I ricattatori, spiega un report di F-Secure che ha sondato l'assistenza di sei diverse famiglie di ransomware, "vogliono fare tutto il possibile per 'aiutare' la vittima a riottenere i file". Non solo: i criminali sono spesso disposti a negoziare i prezzi, abbassando

su richiesta il valore iniziale. Da versare comunque sempre e solo in bitcoin, nel campione esaminato da F-Secure. Anche la scadenza entro cui pagare non è quasi mai tassativa e può essere negoziata.

Il fatto è che si tratta di un settore in continua trasformazione. Nel 2016 erano ben 130 le famiglie di ransomware esistenti, mentre i singoli o i gruppi criminali che ne gestiscono la distribuzione sono sempre più in competizione per una stessa fetta di mercato. Questo ha portato a sviluppare innovazioni su più fronti. Uno di questi è appunto il miglioramento della customer care. Un altro è il potenziamento delle minacce. La campagna dietro al ransomware Jigsaw ha avuto il dubbio merito di lavorare su entrambi i piani, mescolando sadismo e supporto personale. Così, da un lato, ha introdotto un contatore che ogni ora cancella un file finché non viene pagata la cifra indicata (e se l'utente prova a spegnere il pc, vengono cancellati automaticamente mille file per punizione). Dall'altro, alla richiesta di riscatto ha aggiunto un link a una chat live, dove le vittime possono interloquire in diretta con gli aggressori. E in alcuni casi trattare sul prezzo. Una "attenzione al cliente" che però, in questo caso, è anche un modo per convincerlo a pagare pur potendo evitarlo. Tempo prima, infatti, alcuni ricercatori avevano sviluppato uno strumento per la decifrazione gratuita dei file colpiti da Jigsaw. Oppure c'è il caso del software Chimera, che ha introdotto una variante estorsiva ancora più maligna: oltre a cifrare i file, minaccia di diffonderli online se il riscatto non viene pagato. A quel punto avere il backup serve a poco.

Un'altra variazione è il pacchetto ransomware più spyware, software spia. Ad averne individuato alcune istanze sono stati i ricercatori della società maltese ReaQta. Il malware rinvenuto dai suoi analisti cifrava sì i file delle vittime chiedendo circa 250 dollari di riscatto, ma nel contempo scaricava sul loro pc un certo tipo di trojan di nome Pony. Questo software era poi in grado, al di là della estorsione per riavere i file, di restare sul pc per rubare successivamente password e altre credenziali di accesso a siti e servizi. Non è la prima volta che si trovano malware in grado di combinare entrambe le caratteristiche, e qualcuno ha iniziato a parlare di ransomware come "distrazione" per altre operazioni, più di spionaggio o comunque di furto di dati.

I ricercatori di ReaQta, in prima linea sul fronte malware, si sono trovati anche a tracciare e a identificare alcuni dei cyber-criminali che gestiscono

queste ondate di estorsioni. In particolare hanno individuato una campagna che colpiva tre Paesi – Danimarca, Spagna e Italia – e che veniva gestita dall'Ucraina. Gli italiani erano presi di mira attraverso finte mail Sda (Poste Italiane), Telecom Italia ed Enel, fatte abbastanza bene, tranne per l'italiano zoppicante. L'infrastruttura di cyber-estorsioni era piuttosto sofisticata: le mail inviate ad italiani rimandavano a un sito da cui solo chi stava fisicamente in Italia (chi aveva indirizzo Ip italiano) poteva scaricare il malware, in modo da focalizzare gli sforzi solo sui target desiderati. Dai siti sotto il controllo degli attaccanti – siti che simulavano di essere Telecom, Enel o Sda – gli utenti venivano invitati a scaricare un documento o una bolletta o un'etichetta da stampare per ritirare un pacco arrivato in un ufficio postale. In quel modo si infettavano e il ransomware iniziava a cifrare.

"Siamo partiti dalla segnalazione di un cliente, uno dei suoi dirigenti si era preso un ransomware. Gli abbiamo chiesto di inoltrarci la mail e abbiamo visto che era una campagna nuovissima. Siamo poi risaliti fino a un server in Croazia che l'attaccante aveva compromesso con un exploit per poi distribuire da lì i ransomware. In quel modo il sito risultava legittimo, non era individuato come malevolo da servizi anti-spam. Poi, anche a causa di alcuni errori dell'attaccante, siamo risaliti a tutta l'infrastruttura con cui era gestita la campagna, individuando pure l'indirizzo Ip di casa del suo autore", mi spiega il già citato Alberto Pelliccione. Indirizzo che corrisponde a un individuo residente nella città ucraina di Mariupol. Da qui il tizio o il gruppo tirava le fila delle cyber-estorsioni attraverso una catena di comando che comprendeva quattro server in Russia (due da cui distribuiva il ransomware, e due da cui lo controllava); due server in Germania; e uno nella stessa Ucraina. Invece il server croato individuato inizialmente dai ricercatori apparteneva a una persona che non c'entrava nulla, ma era stato sequestrato all'insaputa del suo proprietario dagli estorsori che lo utilizzavano per metterci sopra i siti di phishing. "In questo modo gli utenti non erano mai indirizzati direttamente verso i siti che ospitavano il malware vero e proprio, ma su questi siti intermedi. Così, se uno dei siti di phishing salta, possono rimandare i nuovi utenti al volo su altri finti siti senza perdere quelli, cruciali, che diffondono il software malevolo".

Spieghiamo meglio. I criminali dividono l'infrastruttura in due parti: da

un lato, i siti di phishing che simulano di essere il finto portale Enel, Telecom, ecc., e su cui mandano gli utenti; dall'altro, i siti da cui si scarica il malware vero e proprio, che a volte sono ospitati in servizi cloud. I finti portali di phishing vengono caricati su siti web di persone o aziende ignare, che sono stati "bucati" a causa di vulnerabilità; oppure su finti domini registrati appositamente, che simulano i siti autentici di Enel, Telecom e via dicendo. Ma il malware è collocato altrove, anche su piattaforme come Dropbox o Google Drive. Tale compartimentazione protegge meglio il malware: se i finti siti Enel, Telecom, ecc. vengono individuati e fatti chiudere, i criminali devono solo riaprirne altri simili al volo, su nuovi domini, che puntano poi al malware, rimasto immutato, nel cloud o su altri siti. Ad ogni modo, cosa è successo dopo che avete tracciato a ritroso la campagna e addirittura chi la gestiva?, chiedo a Pelliccione. "Abbiamo informato sia il proprietario del sito che era stato bucato sia le autorità, ma non è successo nulla. La campagna si è fermata per un po', poi è ripartita bucando nuovi siti, questa volta in Perù e in Bolivia. Da lì hanno ripreso a colpire utenti europei".

Sta di fatto che nel 2016 i ransomware sono stati sicuramente il fenomeno cyber-criminale dell'anno. Che non ha risparmiato nessuno. Mentre lavoravo a questo libro, e dopo aver pubblicato vari articoli sul tema, un giorno ho ricevuto la telefonata di un giornalista. "Carola, mi sono preso un ransomware", mi dice subito con voce catacombale. Non solo lui, a quanto pare, bensì un intero gruppetto di suoi colleghi. Non si è mai capito come se lo fossero preso; il dubbio è che potessero aver visitato uno stesso sito malevolo, in grado di infettarli anche senza dover scaricare nulla, attraverso qualche vulnerabilità nel browser. Nessuno di loro alla fine ha pagato: in qualche modo sono riusciti a recuperare una buona parte dei dati cifrati. Intoppo superato, dunque, in tal caso. Tuttavia, considerato che un ransomware può veicolare di nascosto anche un software spia, e che i giornalisti possono essere prede ghiotte di diversi tipi di spionaggio, bisogna fare molta attenzione a questo genere di episodi. E far seguire un controllo approfondito dei sistemi che ne sono stati colpiti.

5.
La cripto-guerra dei vent'anni

Nel cuore delle indagini informatiche

Lo studio di Mattia Epifani sta in un antico palazzo di una via ottocentesca di Genova. Qui i telefonini non prendono a causa dei muri spessi. È il loro ultimo tentativo di fuga, perché i dispositivi che entrano fra queste pareti finiscono nella maggior parte dei casi per non avere più segreti. Anche quando i segreti vorrebbero mantenerli.

Sul tavolo Epifani poggia un'anonima scatoletta scura: è un Forensic Falcon, un duplicatore di dischi, prodotto da Logicube, azienda californiana leader nella realizzazione di apparecchi per la duplicazione di hard disk e l'acquisizione forense. Ci attacchi un disco o un pc da una parte, e dall'altra un supporto di memoria dove vuoi fare una copia perfetta, un clone esatto, disco a disco, bit a bit, che non include solo i file ma anche quanto è stato cancellato o lo spazio non allocato. Poi si schiaccia un pulsante e in breve tempo il disco viene acquisito, copiato. C'è anche una funzione, "write-blocked", che impedisce che il disco collegato possa in alcun modo essere modificato dalla scatoletta.

Mentre legge e trascrive i dati, il dispositivo crea anche una firma digitale dell'hard disk che sta copiando, con un programma di hashing, insieme a un registro delle sue attività. L'hash è un algoritmo che trasforma un certo contenuto in una breve e univoca sequenza di numeri e lettere; ogni cambiamento al contenuto modifica la sequenza; anche un solo bit che muta fa cambiare completamente la firma hash. Per cui l'hashing, calcolando l'impronta matematica dei dati da clonare (il "digest"), garantisce la loro integrità. In pratica è come se si mettesse un sigillo

matematico sullo stato dell'hard disk e dei suoi contenuti, un bollino contro rischi di interpolazioni future. Tale operazione è importante perché garantisce la catena di custodia, documenta cioè la corretta acquisizione e conservazione di dati digitali che potrebbero essere poi usati come elementi di prova.

"Alla fine avrai una immagine forense, una copia di tutte le zone del tuo hard disk o della chiavetta", mi dice Epifani dopo avermi mostrato come funziona il Forensic Falcon. Lui è uno dei massimi esperti italiani di informatica forense, la disciplina che si occupa di individuare, estrarre e conservare dei dati informatici per permettere poi di valutarli come prova in un processo. Esiste uno standard internazionale per identificare, raccogliere e proteggere le prove digitali.

Gli informatici forensi sono spesso laureati in informatica (o in ingegneria informatica), con ulteriori dottorati o specializzazioni, e lavorano molto in ambito processuale, dove possono essere di volta in volta consulenti tecnici del pm, delle parti, dell'imputato; periti del giudice; oppure possono intervenire come ausiliari in perquisizioni e sequestri della polizia giudiziaria. Il loro lavoro è esploso soprattutto negli ultimi anni, ma a renderlo improvvisamente sexy ci ha pensato l'Fbi. Che nel 2016 ha ingaggiato un inedito braccio di ferro con Apple: 43 giorni di scontro mediatico senza esclusione di colpi terminato all'improvviso con una tregua e un aggiustamento tattico.

Lo scontro Fbi-Apple

L'antefatto è il seguente: il 2 dicembre 2015 un attacco terroristico uccide 14 persone a San Bernardino, in California. I due attentatori – marito e moglie – muoiono nello scontro a fuoco con la polizia. Che metterà poi mano sull'iPhone dell'uomo, Syed Rizwan Farook, considerato la mente della strage.

I contenuti del telefono sono però cifrati, e nessuno – nemmeno Apple – è in grado di accedervi senza immettere sul dispositivo il codice di sblocco scelto dal suo proprietario. L'Fbi allora chiede un aiuto alla multinazionale di Cupertino per trovare un modo di accedere al telefono. La soluzione che hanno in mente è di provare un attacco a forza bruta sulla password: significa tentare tanti codici diversi finché non si azzecca quello giusto. C'è

però un problema in questo piano. Gli iPhone progettati da Apple contemplano anche un sistema di sicurezza per evitare di essere preda di simili attacchi. Esiste infatti un meccanismo automatico di autodistruzione dei dati del telefonino che si attiva dopo dieci tentativi falliti di inserire il codice di accesso. E anche se fosse aggirato in qualche modo il limite dei dieci inserimenti, si incontra una seconda barriera: nel caso di ripetute prove di accesso, il telefono inserisce dei tempi di attesa sempre più lunghi per digitare il tentativo successivo.

Le prime richieste avanzate in maniera riservata dai federali non convincono Apple. E allora l'Fbi agisce per vie legali e ottiene una ordinanza da un magistrato federale. È il 16 febbraio 2016 quando inizia un incredibile braccio di ferro tra l'azienda tech forse più famosa al mondo e il governo degli Stati Uniti, la nazione in cui risiede. Esperti di sicurezza di ogni dove aprono Twitter e tirano fuori i popcorn mentre uno dei loro oggetti di studio più esoterici, la crittografia, buca le pagine dei giornali non specializzati.

Cosa chiede l'ordinanza del 16 febbraio? Che il colosso di Cupertino dia all'Fbi un software, scritto appositamente da zero, per disattivare o aggirare i meccanismi di protezione dell'iPhone, in modo da superare il limite dei dieci tentativi. Ma la "ragionevole assistenza tecnica" chiesta dal giudice ad Apple – sulla base, peraltro, di una legge nota come All Writs Act che risale all'anno di grazia 1789 – dovrà anche consentire all'Fbi di inserire i codici sull'iPhone in questione attraverso la porta fisica dell'apparecchio, via Bluetooth o Wi-Fi, cioè attraverso un software. Tutto ciò per evitare di digitare manualmente il codice, cosa che ovviamente sarebbe impraticabile per numerosi tentativi; e per impedire che il dispositivo inserisca tempi di attesa tra i vari inserimenti.

Apple, da azienda leader nel marketing e nella comunicazione, risponde rivolgendosi direttamente ai clienti e ai media. Attraverso una lettera aperta, la casa di Cupertino replica che si tratterebbe di "una decisione senza precedenti che minaccia i nostri clienti". Perché il governo americano le starebbe chiedendo di costruire una "backdoor" per l'iPhone. Le backdoor sono sistemi che consentono di entrare in un computer aggirando i suoi sistemi di identificazione e protezione, come una porta di servizio; e sono l'anatema di qualsiasi esperto di sicurezza informatica. L'Fbi – sostiene Apple – vuole farci creare una nuova versione del sistema

operativo dell'iPhone che aggiri importanti funzioni di sicurezza dello stesso, e poi installarlo sul telefono sottoposto a indagine. "Nelle mani sbagliate questo software – che ad oggi non esiste – potrebbe potenzialmente sbloccare qualsiasi iPhone una volta che sia in possesso di qualcuno".

Per l'Fbi naturalmente non si sta parlando di alcuna backdoor, perché – è la sua tesi – la versione aggiornata e firmata del software realizzato da Apple verrebbe usata e funzionerebbe solo per uno specifico smartphone, quello dell'attentatore, identificato da un unico numero seriale. Apple resterebbe l'unica compagnia al mondo in grado di firmare crittograficamente questo software, che per il giudice potrebbe restare sempre dentro la sede dell'azienda, dove i federali porterebbero il telefono incriminato. E l'Fbi non potrebbe usare lo stesso software per entrare in altri iPhone.

Dal canto suo, Apple replica che tale discorso non è vero. "Una volta creata, la tecnica potrebbe essere usata molte altre volte, su qualsiasi numero di apparecchi. Nel mondo fisico sarebbe equivalente a una chiave maestra ('master key'), capace di aprire centinaia di milioni di lucchetti".

Dalla parte dell'azienda di Cupertino si schierano molte altre imprese tech – tra cui Google, Facebook, Amazon, Cisco, Microsoft, Mozilla, Snapchat, Box, Slack, Yahoo, Intel, AT&T –, gran parte dei crittografi ed esperti di sicurezza e, per una volta, tutto il blocco degli attivisti per i diritti digitali e per la privacy, capitanati da due associazioni importanti, la Electronic Frontier Foundation e la Aclu, storica organizzazione americana di difesa dei diritti civili. "Siamo sicuri che il nostro governo la chiederà [la chiave] ancora e ancora, per altri telefoni, rivolgendo questo potere contro ogni software o apparecchio che abbia l'audacia di offrire una sicurezza elevata. [...] Una volta che una master key è creata, i governi del mondo richiederanno lo stesso da Apple, minando la sicurezza dei loro cittadini", scrive la Electronic Frontier Foundation.

Dello stesso avviso la Aclu. Discuto del caso con uno dei suoi ricercatori di sicurezza informatica, Daniel Kahn Gillmor, dopo averlo incontrato a un evento proprio mentre imperversa lo scontro Fbi-Apple. "Si tratta di un precedente legale nel quale si obbliga un'azienda a produrre un software che verrà poi riconosciuto come legittimo dai suoi stessi apparecchi", mi dice nel corso di una lunga chiacchierata. "Questo ha delle implicazioni a lungo termine molto pesanti. Primo: i sistemi di aggiornamento del

software non saranno più in alcun modo affidabili. Da questi meccanismi potrebbe essere trasmesso di fatto del malware, firmato e garantito dalle stesse aziende produttrici. La prossima volta che il tuo software si aggiorna, ti dovrai chiedere se non si tratti di un potenziale attacco al tuo telefono, firmato e garantito dall'azienda che te lo fornisce e che dice di darti un prodotto sicuro. E non serve essere un criminale o un indagato per pensarlo: potresti essere una minoranza marginalizzata di un Paese democratico, o un giornalista, attivista, avvocato, dissidente in uno Stato autoritario. Secondo: quando crei un simile meccanismo, e un software come quello che è stato richiesto ad Apple, non hai affatto la certezza di poterlo 'contenere'. I dati 'leakano', fuoriescono, sono rubati, hackerati, diffusi, lo sappiamo bene. E finiranno in mano a molti altri soggetti, minando la sicurezza di molti. Terzo: davvero si pensa che altri Stati, a partire da quelli illiberali, non potrebbero chiedere la stessa cosa ad Apple una volta che faccia quel software per il governo Usa?".

Dalla parte dell'Fbi, però, c'è il governo americano, ci sono varie agenzie di sicurezza e, dettaglio non da poco, c'è un'opinione pubblica turbata dal rischio attentati e del tutto a digiuno di sicurezza informatica, per non dire di crittografia. Secondo un sondaggio[19] dell'istituto Pew Research condotto in quei giorni negli Stati Uniti, il 51 per cento degli intervistati riteneva che Apple dovesse aiutare l'Fbi a sbloccare l'iPhone; solo il 38 per cento era contrario (e il resto non aveva un'idea).

Ciò nonostante, Tim Cook, l'ad di Apple, per tutto il tempo appare determinato a tenere il punto sulla questione. È chiaro che l'azienda di Cupertino è pronta a ingaggiare uno scontro legale fino alla Corte Suprema, convinta di poter contare sulla protezione del primo e del quinto emendamento della Costituzione americana. Il primo è quello che protegge la libertà di parola e di espressione. Secondo Apple – ma anche secondo alcuni legali e almeno secondo una precedente sentenza – il software, e la scrittura di un codice, rientrano in questa libertà. Così come il governo non può obbligare un giornalista a scrivere una storia – un esempio citato proprio in una analisi giuridica del caso –, non può nemmeno costringere Apple a scrivere un sistema operativo apposito con la funzione di indebolire la sicurezza dei suoi stessi prodotti. "La richiesta del governo sottopone Apple a un onere senza precedenti e viola i diritti dell'azienda garantiti dal primo emendamento", scrivono i legali di Apple.

La libertà di espressione, come è intesa dalla Costituzione americana, include infatti sia la decisione di dire qualcosa (restando nel caso in questione, la libertà di scrivere un codice) sia la decisione di non dire qualcosa (e quindi di non essere obbligati a dire qualcosa o, come la intendono i legali di Apple, a scrivere un sistema operativo).

Il quinto emendamento tutela il diritto a un giusto processo e il fatto che un privato che non abbia alcuna connessione con un crimine non possa essere arruolato dallo Stato per compiere azioni contrarie ai suoi principi. In pratica, Apple non avrebbe alcuna connessione con la strage di San Bernardino e non può essere obbligata dal governo a creare qualcosa che per di più confligge con la sua attività. Insomma, si parte da una tutela diversa per arrivare a conclusioni simili a quelle del primo emendamento.

Ad ogni modo, il 28 marzo 2016, dopo 43 giorni ai ferri corti, con un colpo di scena, l'Fbi e il Dipartimento di Giustizia abbandonano la causa legale contro l'azienda. La ragione dichiarata è che hanno trovato un modo alternativo di sbloccare l'iPhone, di cui danno pochissimi dettagli. Anche se qualcosa è trapelato. L'Fbi avrebbe pagato circa un milione di dollari per la tecnica che le ha permesso di scardinare i sistemi di protezione dello smartphone di Apple – che era un iPhone 5c con sistema operativo iOS 9. La cifra è approssimativa e non ufficiale, essendo calcolata su una serie di dichiarazioni e precisazioni fatte nel tempo dai vertici dei federali o da varie fonti governative. La somma includerebbe l'utilizzo della tecnica non solo sul telefonino di Farook, ma anche su altri modelli con le stesse specifiche – 5c e stesso sistema operativo, ma non sugli iPhone 6, il cui hardware li rende ancora più resistenti ad attacchi di quel tipo. Tuttavia il governo non avrebbe conoscenza dei dettagli e dei meccanismi profondi dietro al funzionamento di tale tecnica, pur avendone accesso; né potrebbe divulgarli.

Bocche cucite, dunque, su chi sia il fornitore della soluzione. In un primo tempo era stata indicata l'azienda israeliana Cellebrite, in prima linea nello sblocco di telefonini di tutte le marche. Mentre scriviamo, però, la conferma non è ancora arrivata. Non solo: a settembre tre testate giornalistiche – "Associated Press", "Vice Media" e "Usa Today" – hanno iniziato un'azione legale contro l'Fbi per ottenere informazioni sulla transazione. Sapere quanto è stato pagato, per cosa e a chi è d'interesse pubblico, e non può essere tenuto nascosto, è la loro posizione.

Privacy contro sicurezza… o sicurezza contro sicurezza?

Chi ha vinto dunque il braccio di ferro tra Apple e l'Fbi? I federali hanno ottenuto quello che volevano, ma hanno abbandonato il tentativo di cercare un precedente legale sulla questione. D'altra parte, il fatto di aver trovato una soluzione diversa rispetto alla richiesta rivolta ad Apple sconfessa la loro stessa premessa secondo la quale non ci sarebbe stata alternativa.

Il telefonino sbloccato, alla fine, non conteneva dati significativi – ma questo probabilmente è secondario e non si può addebitare ai federali. I quali però, fin dall'inizio, si sono mossi in modo tecnicamente goffo. Ad esempio, hanno commesso un errore senza il quale avrebbero potuto accedere da subito e senza sforzi ai contenuti del telefono di Farook. Questo era infatti connesso a iCloud, il servizio online di backup di Apple. L'uomo non lo aveva più collegato da qualche settimana, ed erano solo quelli i dati che mancavano all'Fbi: quelli precedenti, infatti, li aveva già ottenuti proprio tramite iCloud, perché a quei contenuti Apple era ancora in grado di accedere. Se dunque il telefono di Farook fosse stato connesso a una rete Wi-Fi nota (cioè già usata in precedenza dal proprietario dello smartphone), avrebbe trasferito in automatico tutti i suoi dati non ancora copiati sui server di Apple. Il problema è che un agente, su richiesta degli stessi federali, nelle ore successive al sequestro del telefono, dopo la sparatoria, ha in via precauzionale cambiato la password di iCloud. Così facendo, però, il telefono non avrebbe più fatto il backup automatico. "È stato un errore", ha poi ammesso il direttore dell'Fbi James Comey.

Dal canto suo, Apple nella vicenda si è posizionata come paladina della privacy, nonché come produttrice di apparecchi particolarmente sicuri, più della concorrenza evidentemente. Che si sia trattata di una scelta di puro marketing o anche di mera sopravvivenza sul mercato, è stata portata avanti con determinazione. Certo, a dirla tutta, il suo iPhone (quanto meno quel modello, che non era l'ultimo uscito) non si è dimostrato così inespugnabile, visto che alla fine la soluzione per sbloccarlo e accedervi si è trovata. Ma pur sempre una soluzione da un milione di dollari.

Da una prima analisi, dunque, Apple sembrerebbe uscire dal match come parziale vincitrice, insieme ai suoi clienti, a molti crittografi e agli attivisti

dei diritti digitali. Tuttavia, potrebbe essere una vittoria di Pirro. La ragione è che l'Fbi e il Dipartimento di Giustizia americano sono riusciti a inquadrare la vicenda secondo lo schema sicurezza contro privacy. È importante capire questo schema e la sua forza simbolica per tre motivi. Primo, perché non è nuovo, bensì ricorrente. Secondo, perché è quello che sarà adottato da parte di diversi governi per rafforzare la propria capacità di violare sistemi, dispositivi e comunicazioni, contrastando l'ondata di crittografia forte che negli ultimi anni è tracimata da pochi eletti a milioni di persone. Terzo, perché è tendenzioso, semplificatorio e opinabile.

Qualcuno ha detto che lo scontro Fbi-Apple ha avuto almeno il merito di rendere di dominio pubblico una tensione sotterranea sulla crittografia che va avanti da decenni – anche se a rendere mainstream il dibattito sono stati in realtà gli sviluppi tecnologici e i processi industriali, cioè la diffusione di massa della crittografia forte e la sua disponibilità commerciale. E sono questi che hanno portato a un'intensificazione degli attriti.

La prima cripto-guerra

Negli Stati Uniti governo e tecnologi dibattono della questione almeno dagli anni Novanta, in quella che fu battezzata cripto-guerra. La crittografia – la tecnica che permette a due parti di comunicare in modo sicuro, cifrando i contenuti di un messaggio, rendendolo cioè inintelligibile per chi non conosce la chiave di decifrazione – esiste da secoli in ambito militare, politico e di intelligence. Ma a porre le basi della tensione esplosa negli ultimi anni è stata, nel 1976, l'invenzione della crittografia a chiave pubblica (o asimmetrica) da parte di due ricercatori, Whitfield Diffie e Martin Hellman. Si tratta di un tipo di crittografia di livello militare ma nel contempo facilmente accessibile a cittadini e aziende, basata su una coppia di chiavi, una pubblica e una privata[20].

In pratica lo Stato aveva perso il monopolio della capacità di cifrare in modo davvero robusto. Al punto che, già alla fine degli anni Settanta, alcuni membri del governo Usa si interrogarono su come risolvere quello che a loro avviso era il problema della crescente diffusione della crittografia. Tuttavia, è solo a metà degli anni Novanta che la questione è diventata incandescente, quando la Casa Bianca ha provato a introdurre il

Clipper Chip.

Si trattava di un microchip sviluppato da ingegneri governativi che doveva essere inserito in dispositivi come i telefoni. Il suo intento dichiarato era di fornire degli strumenti di cifratura forte per proteggere le comunicazioni degli utenti senza sacrificare la capacità delle forze dell'ordine e dell'intelligence di accedere a una versione non cifrata dei contenuti. Per ottenere un simile risultato, questa tecnologia avrebbe adottato un sistema di deposito di garanzia delle chiavi, dove una copia della chiave (in quel caso unica) di cifratura/decifratura di ogni chip sarebbe stata conservata dal governo, o da una terza parte certificata dallo stesso. La proposta dell'allora amministrazione Clinton incontrò però la fiera opposizione di tecnologi, difensori dei diritti e dell'industria, e alla fine venne rigettata.

Parallelamente a questa vicenda, si consumò anche uno scontro sulla classificazione della crittografia forte: il governo americano voleva inquadrarla come una tecnologia militare e limitarne le esportazioni. Ma di fronte al rischio di perdite economiche conseguenti a tale decisione, e al fatto che comunque era improbabile limitare la diffusione della crittografia all'estero, i controlli sulle esportazioni sono stati a mano a mano allentati fino a scomparire nel 1999.

La disponibilità di una crittografia robusta ha posto le basi per l'espansione dell'economia digitale e delle comunicazioni online, per protocolli e servizi web cifrati che hanno reso possibile l'e-banking, i pagamenti online, la digitalizzazione del sistema sanitario, la gestione in Rete di attività lavorative delicate e così via. Non solo: "ha rafforzato la protezione delle comunicazioni individuali e migliorato la cyber-sicurezza", hanno scritto nel 2015 gli autori di un saggio accademico significativamente intitolato: "Condannati a ripetere la storia? Lezioni dalle cripto-guerre degli anni Novanta"[21]. I tre autori del saggio ribadiscono come il consenso sulla utilità della cifratura forte in termini di protezione della privacy, della libertà e della stessa sicurezza, negli ultimi anni sia nuovamente minacciato. Come ha commentato al riguardo il noto ricercatore Bruce Schneier, riferendosi proprio ai rigurgiti anti-cifratura degli ultimi tempi: "La seconda cripto-guerra sarà più dura e cattiva e sono meno ottimista che la crittografia forte vincerà nel breve periodo".

La preoccupazione di Schneier non è mal posta, soprattutto se si guarda

con attenzione a quanto accaduto negli ultimi dieci anni o poco più. Dopo il Patriot Act firmato da George W. Bush nella fase successiva agli attentati alle Torri Gemelle – ovvero dopo la prima legge che aumentò i poteri di sorveglianza del governo americano sulle comunicazioni –, nel 2003 il Dipartimento di Giustizia propose un Patriot Act 2, che riguardava proprio la cifratura, prevedendo tra le altre cose una pena minima aggiuntiva di cinque anni per ogni reato in cui fosse usata la crittografia per nascondere informazioni o comunicazioni incriminanti. La proposta non passò, ma le preoccupazioni statali sul tema non svanirono affatto. Già nel 2008, ad esempio, il direttore dell'Fbi Robert Mueller parlava del rischio di "going dark", espressione con cui si fa riferimento alla difficoltà per le forze dell'ordine di accedere a certi tipi di comunicazioni/informazioni a causa degli sviluppi tecnologici.

Nel 2012 i federali tornarono alla carica proponendo una legge che obbligasse i fornitori di mail, app di messaggistica, social network e VoIP (Voice over IP), tipo Skype, a modificare i propri servizi in modo che fossero facilmente accessibili per intercettazioni. La proposta però non convinse Obama e cadde nel vuoto.

Un conto però è il piano della politica, più pubblico; un altro quello che accade dietro le quinte. Così, grazie alle rivelazioni di Edward Snowden, l'ex consulente della Nsa che ha svelato i programmi di sorveglianza americani, nel 2013 si venne a sapere che la stessa Nsa era attivamente impegnata a far adottare standard crittografici deboli o bacati in modo da trarne vantaggio. Non solo: alcuni suoi progetti, come quello dal nome in codice Bullrun, lavoravano a stretto contatto con aziende tecnologiche allo scopo di costruire degli accessi ai loro prodotti. "In alcuni casi, le aziende sono state obbligate dal governo a consegnare le loro master key di cifratura o a inserire una backdoor", scrisse all'epoca il "New York Times".

Uno scontro mai sopito

In questo quadro il Datagate – le rivelazioni sui programmi di sorveglianza statunitensi e non solo – si è abbattuto come una tempesta tropicale in una città del Nord Europa. Tra i suoi effetti, c'è stato il risveglio improvviso di molte società tecnologiche, accusate di collusione con le attività di

sorveglianza dei vari Grandi Fratelli. Affrancate dall'obbligo di riservatezza su quei programmi, rafforzate dall'opinione pubblica improvvisamente resa consapevole, e soprattutto preoccupate per le conseguenze economiche dello scandalo, le aziende hanno iniziato una sorta di escalation tecnologica per rafforzare la privacy e la sicurezza dei propri utenti.

Uno dei passaggi cruciali è stata la decisione di Apple, nel settembre 2014, di fare in modo che iOS 8, la nuova versione del suo sistema operativo mobile, includesse la cifratura disco di default, legandola all'azione dell'utente di inserire un codice di accesso al telefono. A quel punto, se il codice era abbastanza lungo, nessuno – nemmeno la Mela morsicata – sarebbe stato in grado di accedere ai contenuti del telefono. Poco dopo anche Android, il sistema operativo mobile promosso da Google, ha annunciato che la cifratura disco sarebbe presto diventata una sua impostazione predefinita. Anche se questa promessa si è poi scontrata con le resistenze dei produttori di hardware su cui gira Android, preoccupati per le relative complicazioni, e si è infine avverata soltanto nel 2015 per Android 6.0.

"Ora che le rivelazioni di Snowden hanno sottolineato quanto siano vulnerabili i nostri dati, aziende come Apple e Google, che sono state tratteggiate come collaboratrici della Nsa nei primi documenti diffusi, sono nuovamente motivate a dimostrare la loro indipendenza e a competere fra di loro sulla privacy", scriveva nel 2014 il noto giornalista tech Kevin Poulsen. "Indipendentemente da come ci è arrivata, Apple ha raggiunto il posto giusto".

L'editorialista però mostrava anche come questa mossa avesse creato nervosismo in molti apparati statali. Qualcuno già proponeva che Apple e Google – lasciando pure da parte l'idea della backdoor, ritenuta in effetti poco raccomandabile – inventassero una "golden key" (chiave dorata) sicura, per permettere alla polizia di decifrare i dispositivi con un mandato. Che cosa è una golden key? Il concetto non è molto chiaro: probabilmente chi usa questa espressione intende una sorta di master key. Di fatto, l'unica vera differenza tra backdoor e chiave dorata è che la prima tende ad essere una "via d'accesso" nascosta, mentre l'altra sarebbe in qualche modo riconosciuta e legittimata, magari anche certificata (ricordate il Clipper Chip degli anni Novanta?). Non si capisce dunque, per dirla sempre con Poulsen, "perché questa 'chiave dorata' debba essere meno vulnerabile ad

abusi di qualsiasi altra backdoor. Forse è il nome, che sembra un prodotto dello stesso marchio che ha portato il governo cinese a rinominare come ‘scudo dorato’ il suo sistema di censura di Internet. Del resto, come fa a non piacere? Tutti amano l’oro!”.

Nel contempo, si sono diffuse app di messaggistica che hanno introdotto la crittografia cosiddetta “end-to-end”, dove “end” sta per “endpoint”, vale a dire un apparecchio connesso a internet. Quindi un tipo di crittografia che va direttamente da dispositivo a dispositivo. È considerato il livello di cifratura più sicuro a disposizione per chi debba inviare messaggi perché solo i due utenti che comunicano hanno le chiavi per cifrarli e decifrarli: neppure l’azienda che gestisce il servizio può dunque leggerli.

Anche questa applicazione della crittografia ha prodotto malumori in certi ambienti, e già nel settembre 2015 era emerso un primo accenno di baruffa tra Apple e l’Fbi. La casa di Cupertino aveva detto a un tribunale americano che non poteva dare seguito a un mandato di intercettazione in cui si chiedeva di consegnare messaggi inviati via iMessage, la app di messaggistica dell’iPhone, perché appunto erano cifrati end-to-end. E non era nemmeno il primo caso. Ma quella volta, secondo il “New York Times”, il Dipartimento di Giustizia aveva avuto la tentazione di provare un agguato legale per modificare gli equilibri sulla crittografia. Come abbiamo visto, quella strada verrà tentata due mesi dopo, in seguito alla strage di San Bernardino. Ad ogni modo, tornando alle app di messaggistica, iMessage non è la sola, bensì in compagnia di altre, come Signal o Telegram, tutte in rapida diffusione (e variamente affidabili), inclusa quella che ha davvero fatto la differenza per numero di utenti: WhatsApp.

Sebbene avesse iniziato a introdurre la crittografia end-to-end già a fine 2014, la popolare e trasversale app di messaggistica ha annunciato di aver completato la blindatura di tutti i contenuti scambiati fra i suoi utenti proprio durante lo scontro Fbi-Apple. “Tim Cook è il mio eroe”, avrebbe detto uno dei due fondatori di WhatsApp, Brian Acton, all’altro, Jan Koum, durante i giorni della crisi, quando l’ad di Apple non retrocedeva di un millimetro davanti alle pressioni del Dipartimento di Giustizia.

Poche settimane dopo, WhatsApp ha confermato che la migrazione alla forma più forte di cifratura era ormai compiuta del tutto. Per tutti gli

utenti, ovvero per un miliardo di persone nel mondo, messaggi, telefonate, foto, video trasmessi attraverso il servizio erano da allora cifrati end-to-end. Su tutti i tipi di sistema operativo e dispositivi. In chat a due o di gruppo. “In pratica, come Apple, WhatsApp sta facendo saltare i ponti col governo federale”, commentava la rivista “Wired”, “ma lo sta facendo da un fronte molto più ampio che copre circa un miliardo di apparecchi”. Già, perché in questa maniera neanche gli impiegati dell’azienda possono leggere i dati inviati attraverso il suo network: e ciò significa che, anche di fronte al mandato di un giudice, WhatsApp non è in grado in alcun modo di ricavare quei contenuti.

Il sogno cripto-anarchico di portare la crittografia alle masse è stato infine realizzato dalla app di riferimento di adolescenti e gruppi di mamme, per di più ormai acquisita da Facebook. In breve tempo, i più agguerriti tecnosnob si sono ritrovati a usare le telefonate cifrate di WhatsApp perché funzionavano meglio di altri servizi più di nicchia. Ovviamente, non sono mancate conseguenze.

Nel marzo 2016 – proprio mentre Apple aveva il suo bel daffare con l’Fbi – in Brasile un giudice ha mandato in prigione (per 24 ore) Diego Dzodan, il vicepresidente di Facebook per l’America Latina, perché WhatsApp non aveva condiviso con la polizia i messaggi di alcuni narcotrafficanti. Per lo stesso motivo, due mesi dopo, il medesimo giudice ha chiesto alle compagnie di telecomunicazioni di bloccare l’app di messaggistica in tutto il Paese, dove aveva ben 100 milioni di utenti – una messa al bando rigettata dopo 24 ore da una corte superiore. Ma seguito da un altro blocco temporaneo a luglio.

Peraltro, in Gran Bretagna, già nel gennaio 2015 il primo ministro David Cameron aveva annunciato di voler mettere fuori legge tutte quelle comunicazioni che non possono essere lette dai servizi di sicurezza, anche qualora siano muniti di mandato. Molti all’epoca si sono interrogati su questa uscita: vuole davvero vietare iMessage, Signal, WhatsApp e via dicendo? E come intende farlo?

A questo punto è abbastanza chiaro che le pressioni sulle aziende tech per introdurre backdoor o fornire le chiavi di decifrazione o indebolire i sistemi di protezione non sono mai scomparse dagli anni Novanta. Quella che dunque è stata ribattezzata come seconda cripto-guerra, in riferimento alle tensioni degli ultimi anni sulla crittografia, va piuttosto interpretata

come un unico lungo conflitto a bassa intensità che prosegue dagli anni Novanta, con alcuni momenti in cui erompe in superficie.

Lo spettro delle backdoor

Più recentemente, a moltiplicare gli scontri sono stati due fenomeni: da un lato, l'emergenza terrorismo (su cui torneremo); dall'altro, la naturale adozione della crittografia forte da parte delle aziende tecnologiche. Uso appositamente la parola "naturale", perché sebbene abbia giocato un ruolo l'effetto Snowden, la tendenza a rendere più sicure comunicazioni e informazioni sarebbe stata probabilmente inevitabile, forse solo più lenta. E la ragione di questo trend è molto semplice: da un lato, è diventato tecnologicamente possibile; dall'altro, è assolutamente auspicabile. Perché agli occhi di tutti – inclusi ormai anche gli utenti comuni – è chiaro che stiamo velocemente e pericolosamente trasferendo le nostre esistenze in un ambiente digitale insicuro. Dannatamente insicuro.

La comunità di esperti di sicurezza informatica e di crittografi è fortemente orientata a rigettare qualsiasi genere di backdoor. Nel luglio 2015, 14 tra i principali specialisti del settore hanno scritto un saggio fondamentale sul tema, intitolato "Chiavi sotto lo zerbino: obbligare all'insicurezza con la richiesta governativa di accedere a tutti i dati e le comunicazioni"[22]. Molti degli autori del saggio sono gli stessi che hanno osteggiato il Clipper Chip di Bill Clinton. Ora, esattamente vent'anni dopo, tornano alla carica e senza peli sulla lingua, in una sorta di déjà-vu.

La tesi del loro articolo è che dare a un governo un accesso eccezionale a comunicazioni cifrate non sia tecnicamente fattibile, senza mettere in pericolo dati riservati e infrastrutture critiche. Affidare allo Stato le chiavi per aprire comunicazioni cifrate, oltre a richiedere una straordinaria fiducia nello stesso, esporrebbe queste chiavi al rischio di essere sottratte o abusate da terze parti. Tanto più che attacchi informatici a organismi statali anche delicati sono quasi all'ordine del giorno. Infine, se gli Stati Uniti o la Gran Bretagna imponessero delle backdoor alle aziende tech, cosa impedirebbe a tutti gli altri Stati – dalla Cina in giù – di fare altrettanto?

Nell'ottobre 2015 l'amministrazione Obama sembrava avere accantonato i tentennamenti al riguardo, decidendo di non fare una legge per forzare le compagnie tecnologiche a creare backdoor. Due mesi dopo, con la strage

di San Bernardino, è iniziato il braccio di ferro con Apple. E un nuovo ciclo della cripto-guerra è ripartito. Con la differenza che oggi l'ansia per il terrorismo internazionale è probabilmente al suo apice.

I dispositivi non sono fortezze

Torniamo di nuovo nello studio genovese di Mattia Epifani, l'esperto di informatica forense. Prende una valigia grossa, pesante, la ripone sul tavolo e la apre. Dentro ci sono decine di attacchi per telefonino e cavi per microUsb, ordinatamente inseriti nelle loro guide. Un kit che costa intorno agli ottomila euro e che, insieme ad alcuni software, ti dà la possibilità di accedere a una buona parte dei contenuti di quasi tutti gli smartphone.

Sì, è come avete letto. Perché malgrado tutti i discorsi appena fatti sulla crittografia, e sullo scontro Fbi-Apple, la verità è che la cifratura usata dagli smartphone per proteggere i dati conservati sul dispositivo non è un sistema infallibile. A livello matematico e teorico lo è. Ma poi c'è l'implementazione pratica: dell'hardware, del software e dell'uso da parte dell'utente. Le falle dunque esistono eccome, e possono essere a livello software, hardware o di tipo più "concettuale", attraverso i sistemi di backup nel cloud o sul pc. Tre piani diversi dove si possono commettere errori; lasciare bachi; o contro cui condurre attacchi. Senza mettere in conto l'utilizzo fatto dall'utente, dove le imperfezioni e gli errori si moltiplicano.

Ci sono aziende specializzate esclusivamente nello sblocco degli smartphone. Le quattro principali sono Cellebrite (israeliana), Msab (svedese), ElcomSoft e Oxygen (russe). "Possono acquisire i dati da migliaia di modelli di telefonini", mi spiega Epifani. L'osso duro allo stato attuale sono gli iPhone dal 5s in avanti, che rendono particolarmente difficile a livello hardware l'estrazione e l'interpretazione del chip. E però devono avere anche l'ultimo sistema operativo mobile di Apple nonché un pin di sblocco di almeno sei caratteri. E oltre a ciò, l'utente deve comunque essere in grado di prendere anche altre precauzioni.

Ma è una situazione temporanea. "Apple ha imparato tantissimo, tuttavia le vulnerabilità o i modi per violare gran parte dei telefoni probabilmente si continueranno a trovare", commenta Epifani. "In ogni caso, non ha senso

chiedere alle aziende di violare il loro sistema o di indebolire la loro cifratura. Bisogna anche tenere presente che comunque l'elemento digitale è d'aiuto alle indagini ma non è quasi mai esclusivo o risolutivo, a parte forse in casi di criminalità informatica, dove però conta più il pc del telefono".

[19] http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

[20] Si cifra un messaggio indirizzato a qualcuno utilizzando la sua chiave pubblica (che appunto può essere divulgata), e il destinatario decifrerà il messaggio ricevuto usando la propria chiave privata (che invece si tiene nascosta).

[21] https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.

[22] https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

6.
Reti di terrore

Paura e controllo

"Siamo di fronte a una nuova minaccia. Bisogna che le aziende tecnologiche capiscano che hanno un ruolo importante da giocare". A parlare è il ministro dell'Interno francese, Bernard Cazeneuve. È il febbraio 2015, poche settimane dopo gli attacchi terroristici alla redazione del giornale "Charlie Hebdo" e al supermercato kosher. La dichiarazione del ministro anticipa quello che sta per andare a chiedere ai manager della Silicon Valley, salendo su un aereo diretto negli Stati Uniti.

Le questioni che Cazeneuve e altri politici europei e americani stanno mettendo sul piatto da tempo sono due: la prima riguarda la gestione di contenuti estremisti in Rete e sui social network; l'altra ha a che fare con la cifratura dei servizi e delle app. Per i funzionari dell'intelligence e alcuni politici, le imprese digitali dovrebbero fare di più, molto di più di quanto non stiano facendo. Cosa sia esattamente questo di più, in concreto, non è però affatto così chiaro. E gli incontri a porte chiuse tra rappresentanti governativi, agenzie di sicurezza e legali di società private non aiutano a capire.

Il fatto è che i principali colossi tech stanno collaborando da tempo, in vario modo, con le autorità, rimuovendo contenuti e fornendo, quando possibile, i dati su utenti sotto indagine. Proprio in occasione degli attacchi di gennaio in Francia, Microsoft ha passato alla polizia i contenuti della casella di posta dei fratelli Kouachi nel giro di 45 minuti. E quando il video del poliziotto francese ucciso dal terrorista, sempre durante gli attacchi di gennaio, ha iniziato a girare online, Google si è attivata in pochi minuti per rimuoverlo da YouTube. Secondo dati della stessa azienda, nel 2014 la casa di Mountain View avrebbe eliminato 14 milioni di video che mostravano

incitamento all'odio e alla violenza o varie efferatezze.

Eppure, non sono mancate le volte in cui alcune di queste piattaforme sono state indicate come facilitatrici del terrorismo, se non direttamente responsabili. Un clima che ha portato addirittura a una causa legale. Nell'agosto 2016 un giudice della corte distrettuale di San Francisco ha rigettato una causa contro Twitter in cui la piattaforma veniva accusata di aver fornito "supporto materiale" ai terroristi dell'Isis. A muovere l'azione legale i famigliari di un contractor americano, ucciso in Giordania da un terrorista. Secondo i querelanti, l'assassino sarebbe stato ispirato dalla propaganda estremista diffusa via Twitter. E il social network sarebbe stato responsabile per aver fornito account ai sostenitori dei terroristi e per non aver "individuato e prevenuto" la diffusione dei loro tweet. Il magistrato ha però respinto le accuse, anche perché la piattaforma è protetta da una legge nota come Safe Harbor (una sezione del Communications Decency Act). Si tratta di una clausola che protegge i servizi online dalla responsabilità legale per i contenuti pubblicati sui loro network (mentre ne sono responsabili gli autori, cioè gli utenti). Il caso contro Twitter però è interessante perché mostra la pressione cui sono sottoposte le aziende tech a causa del loro ruolo sociale.

Il rapporto tra Isis e Rete è stato sviscerato in lungo e in largo, e meriterebbe una discussione a parte. Ma mi preme sottolineare un punto metodologico: malgrado la quantità di commenti, analisi, saggi, articoli sulla questione, ci sono a mio avviso pochi dati ed elementi fattuali a disposizione. Questo fa sì che le stesse analisi siano contraddittorie e che sia difficile misurare il peso specifico dei singoli fenomeni narrati. Di conseguenza il tema, anche per la sua drammaticità, viene facilmente ideologizzato.

Come scrive Neil Johnson, un fisico americano che ha studiato e analizzato quasi 200 comunità online di simpatizzanti pro-Isis sul social network russo VKontakte, "all'inizio del nostro lavoro, abbiamo condiviso i primi risultati con persone dell'intelligence, ma sospetto che non fossero del tutto a loro agio con il nostro approccio scientifico dei sistemi complessi. La comunità dell'intelligence sembra dominata da scienziati sociali che preferiscono discussioni narrative e teorie sul comportamento umano, mentre il nostro lavoro era basato sui dati".

Le tre direttrici del dibattito Isis/Internet

In attesa che questo atteggiamento cambi e che si moltiplichino studi mirati sul tema, è interessante sottolineare le tre direttrici su cui si è sviluppato il dibattito Isis/Internet fino ad oggi: la Rete come piattaforma di propaganda/radicalizzazione/reclutamento; la Rete e la crittografia come strumenti per nascondersi, sparire (going dark), comunicare senza essere facilmente intercettati; la Rete come veicolo diretto di attacco (cyber-Califfato, hacker dell'Isis, cyber-terrorismo).

Come abbiamo visto, la prima direttrice ha coinvolto soprattutto i colossi tech: Google, Facebook, Twitter, ecc. In particolare, il social da 140 caratteri è stato spesso preso di mira per l'utilizzo intensivo che ne facevano i sostenitori dell'Isis. Utilizzo che però tra 2015 e 2016 sembra essere diminuito. Il traffico Twitter dell'Isis – e quindi la conseguente propaganda – sarebbe infatti crollato del 45 per cento negli ultimi due anni, in base a quanto riferito dalla stessa amministrazione americana nel luglio 2016. Secondo alcuni dati dell'agenzia "Associated Press"[23], nell'estate 2016 un profilo Twitter pro-Isis aveva in media 300 seguaci ("follower"); due anni prima la cifra era di 1500.

Il calo di follower è probabilmente dovuto alla chiusura forzata di account di quel tipo da parte della piattaforma, che ha rafforzato i team dedicati alla revisione di contenuti estremisti (introducendo anche tecnologie di filtro, come quelle per contrastare lo spam), per cui, anche se i profili sono riaperti con nuovi nomi utente, non riescono a ritessere in poco tempo i rapporti online precedenti. Il social dei cinguettii ha detto di aver sospeso oltre 125mila profili di questo tipo da metà 2015 al febbraio 2016, e altri 235mila nei sei mesi successivi, anche se ribadisce come non ci sia "alcun 'algoritmo magico' per identificare contenuti terroristici su Internet, per cui le piattaforme online globali sono obbligate a compiere scelte difficili basate su poche informazioni e indicazioni".

In realtà, il risultato – almeno nei tweet in lingua inglese – è stato palpabile. E ha in parte causato uno spostamento dei pro-Isis da Twitter ad altri luoghi online, a partire da Telegram. Per il grande pubblico l'Isis è diventato dunque meno visibile ma non è sparito dalla scena: si è raccolto in circoli più ristretti sui gruppi e i canali delle app di messaggistica.

Il dibattito sulla Rete come ambiente di radicalizzazione e successivo

reclutamento non nasce certo con l'Isis. Anche se l'appiattimento sull'attualità dei media – che stanno guidando la discussione pubblica sul terrorismo – tende a tralasciare un semplice fatto. Ovvero che Internet – e il terrorismo nell'era di Internet – esistono da molti anni, ben prima del Califfato. "Senza dubbio, Internet è la sede più importante per reclutare la gioventù islamica", diceva il generale di brigata dell'esercito John Custer, capo dell'intelligence al comando centrale per l'Iraq e l'Afghanistan.

Era il 2007. L'episodio è riportato nel libro *L'odio online* di Giovanni Ziccardi, che riprende anche uno studio Rand del 2013 proprio sul ruolo della Rete nella radicalizzazione dei terroristi: non è provato "l'assunto che Internet sostituisca l'esigenza degli individui di incontrarsi di persona durante il processo di radicalizzazione: la Rete sembra essere più che altro complementare alla comunicazione di persona", scrive Ziccardi. "Non è neppure documentabile che Internet abbia contribuito alla self-radicalisation, dal momento che in tutti i casi analizzati i soggetti avevano preso contatti con altri individui, fisici o virtuali".

Il Califfato viene proclamato nel 2014. Forse ha cambiato questo scenario? Difficile verificarlo con certezza. Il punto è che, malgrado l'attenzione mediatica e il continuo riferimento alla Rete come fabbrica di potenziali terroristi, ci sono pochi dati sul fenomeno. Nell'estate 2016 sono però uscite due analisi che provano a quantificare la radicalizzazione online e che giungono a una conclusione simile. Quella secondo cui il ruolo della Rete rischia di essere sopravvalutato.

La prima è un articolo firmato da Seamus Hughes del Programma sull'estremismo della George Washington University, insomma un nome autorevole in questo campo: e il titolo è inequivocabile: "Per fermare il reclutamento dell'Isis, concentratevi offline"[24].

In pratica – sostiene l'autore – mentre l'ubiquità della propaganda via social media dell'Isis è evidente, il suo effetto è più controverso. Il ruolo di Internet in questo senso, sebbene reale, è sovrastimato. E se si vuole fermare il reclutamento, è necessario fermare i contatti di persona. La tesi deriva dall'analisi di 100 casi legali legati all'Isis negli Stati Uniti, dai quali emerge che sono gli amici, le famiglie e i partner a influenzare tangibilmente il processo di radicalizzazione. Mentre un numero molto limitato di radicalizzazioni di simpatizzanti è avvenuto esclusivamente nel dominio digitale.

“Nessuno nega che Internet abbia un ruolo e che faciliti contatti. Tuttavia sono soprattutto nuclei radicalizzati offline che trascinano altri alla mobilitazione”, mi ha detto Lorenzo Vidino, direttore del Programma sull’estremismo della citata università americana e membro della commissione di studio di Palazzo Chigi su radicalizzazione ed estremismo jihadista in Italia, in un articolo per “La Stampa”. “Lo studio è sugli Stati Uniti, ma per l’Europa questo vale ancora di più. Se guardiamo alla mobilitazione dei ‘foreign fighter’ in Paesi come Belgio, Francia, Danimarca e Germania, vediamo che questa non è distribuita omogeneamente sul territorio, ma va per aree, città, ecc. Ciò avviene perché ci sono nuclei di soggetti radicalizzati che ne trascinano altri: insomma si parte per la Siria perché si conosce qualcuno”.

L’altro studio, uscito quasi in contemporanea, riguarda la Spagna, e ha analizzato i detenuti per attività legate al jihadismo a partire dal 2013. Per quanto riguarda l’ambiente di radicalizzazione, l’online ha pesato nel 18,4 per cento dei casi; contatti e luoghi esclusivamente offline hanno contato per il 28,9 per cento; mentre in un 53 per cento di casi nel processo di radicalizzazione sono presenti sia canali virtuali che fisici, con social network e Facebook a farla da padrone nell’ambito online.

La seconda direttrice del dibattito è quella della cifratura e del suo ruolo nella crescita delle potenzialità dei terroristi. Ed è ancora più controversa. Subito dopo la serie coordinata di attentati terroristici di Parigi del novembre 2015 – quelli che hanno colpito il teatro Bataclan e altri luoghi cittadini, uccidendo 130 persone –, il “New York Times” uscì con un articolo in cui, citando fonti dell’intelligence francese, spiegava come gli attaccanti avessero usato comunicazioni cifrate per coordinarsi con l’Isis. Tuttavia successivamente la testata ha riformulato il pezzo, spiegando che i funzionari europei non avevano mostrato prove per quella affermazione. Al contrario, era emerso in modo sostanziale che alcuni degli attentatori si conoscevano da tempo e si incontravano di persona, abitavano nella stessa area geografica, ed erano noti all’intelligence e alle forze dell’ordine di diversi Paesi.

Questo non ha impedito ai media di individuare in Internet uno dei principali responsabili del massacro: crittografia, bitcoin, Dark Web e la Play Station (in particolare il suo sistema di comunicazione cifrato) sono stati tutti tirati in ballo da commentatori o da fonti spesso anonime,

divenendo nell'immediato il facile capro espiatorio delle falle investigative. E ciò malgrado l'esiguità delle prove a loro carico. Intanto, l'ex direttore della Cia James Woolsey era arrivato ad affermare in varie interviste che Edward Snowden, la fonte del Datagate e delle rivelazioni sulla sorveglianza di massa, aveva le mani sporche di sangue delle vittime francesi. Perché, a suo dire, le informazioni rivelate sulla Nsa e su altre agenzie avrebbero messo in allerta criminali ed estremisti, facendogli prendere contromisure rispetto ai sistemi usati dalle intelligence occidentali.

Eppure i terroristi usavano la crittografia da almeno 15 anni. Al-Qaeda nascondeva le proprie comunicazioni attraverso vari sistemi di cifratura, inclusa la steganografia – l'utilizzo di immagini in cui nascondere altre informazioni – fin dalla fine degli anni Novanta, mimetizzando documenti anche dentro immagini porno. "Bin Laden, accusato delle bombe alle ambasciate americane dell'Africa orientale nel 1998, e altri della sua organizzazione nascondono mappe e foto di obiettivi degli attentati e pubblicano istruzioni per attività terroristiche su chat di sport, forum pornografici e altri siti web, spiegano fonti governative", scriveva "Usa Today" nel lontano 2001, prima ancora dell'attentato alle Torri Gemelle, riferendosi proprio alla steganografia.

Sempre dallo stesso articolo, vale la pena riportare un lungo brano: "Una cifratura impossibile da rompere sta permettendo ai terroristi – Hamas, Hezbollah, al-Qaeda e altri – di comunicare le loro intenzioni criminali senza temere intrusioni esterne, ha detto il direttore dell'Fbi Louis Freeh lo scorso marzo durante una testimonianza a porte chiuse davanti a una commissione del Senato: 'Stanno bloccando i nostri sforzi come forze dell'ordine di individuare, prevenire e investigare attività illegali'. Un tempo esclusivo dominio della Nsa, l'agenzia americana supersegreta incaricata di scrivere e soprattutto di rompere codici elettronici, la cifratura è diventata lo strumento quotidiano per estremisti musulmani in Afghanistan, Albania, Gran Bretagna, Kashmir, Kosovo, Filippine, Siria, Stati Uniti, Cisgiordania, Striscia di Gaza e Yemen, affermano funzionari statunitensi. È diventata così fondamentale nelle operazioni di questi gruppi che Bin Laden e altri estremisti musulmani la insegnano nei loro campi in Afghanistan e Sudan, aggiungono". Ribadiamo: lo scriveva "Usa Today" nel 2001.

I membri più radicati all’interno dei gruppi terroristici hanno dunque sempre adottato sistemi per nascondersi e schermare le proprie informazioni. Quella che a livello investigativo ha forse fatto la differenza è stata la diffusione di massa di una crittografia forte e semplice da utilizzare, come abbiamo visto nel precedente capitolo. A partire da app usate per comunicare a 360 gradi, come WhatsApp o Signal, che permettono sia di scambiare messaggi, foto e video, sia di parlare a voce. E tutto resta solidamente cifrato. La conseguenza è che rimane più difficile origliare e scremare preliminarmente le informazioni sull’ambiente circostante ai terroristi.

“Posso capire la preoccupazione crescente degli investigatori”, mi dice Stefano Zanero, professore di sicurezza informatica al Politecnico di Milano, e convinto sostenitore del fatto che la crittografia non si possa o debba limitare. “Quando colpisci il terrorismo ti occupi anche di un popolo di fiancheggiatori e simpatizzanti: si tratta di un tipo di persone più collaterali ma utili alle indagini, che una volta era più facile intercettare perché non arrivavano ad adottare le precauzioni di chi era più operativo. Oggi anche loro usano canali cifrati”. A lamentare le difficoltà incontrate a causa della cifratura è stato, nel marzo 2015, anche il direttore dell’Europol, Rob Wainwright.

Dato per buono che, dal punto di vista dell’antiterrorismo (e in genere di chi indaga crimini pesanti), la migrazione dall’uso delle telefonate Gsm – una manna per chi deve intercettare – ad app cifrate end-to-end costituisca effettivamente un problema, il punto è: quali sono le soluzioni investigative più adatte a risolverlo? Ne esistono diverse in realtà. E la comunità tecnologica, nella sua stragrande maggioranza, risponderà che attaccare, indebolire o bandire la crittografia non è una strada percorribile né auspicabile.

“La battaglia sulla crittografia va avanti da anni e non si è mai fermata”, continua Zanero. “Quando i governi hanno capito che non si poteva tenere nel cassetto un pezzo di disciplina scientifica, allora hanno provato a tenerla lontana dal grande pubblico. Eppure la diffusione della cifratura è stata positiva, ha spostato più in alto il livello di rischio per tutti gli utenti, permettendo di aumentare la protezione per chi se lo merita, ovvero per la maggioranza delle persone che la usano per attività lecite e importanti. I criminali adottavano la crittografia anche quando era difficile, e

continueranno a farlo anche se dovesse essere illegale”.

Malgrado ciò, nell’agosto 2016 il ministro dell’Interno francese Cazeneuve è tornato all’attacco, proponendo una iniziativa europea per contrastare la cifratura forte delle comunicazioni, la stessa adottata da WhatsApp e soci. All’annuncio è seguito un incontro con il suo omologo tedesco Thomas de Maizière. L’intento di Cazeneuve era di porre le basi europee per “un progetto più internazionale”. Secondo il ministro, molti messaggi scambiati dai terroristi sarebbero ormai cifrati e l’intelligence farebbe fatica a intercettarli. Dunque la questione della cifratura, per il governo francese, sarebbe centrale nella lotta al terrorismo.

Ma cosa aveva in mente il governo di Parigi? Non era chiaro all’epoca. Però la strada delle backdoor era già stata sconsigliata perfino dalla stessa Europol, che nel maggio 2016, insieme all’Enisa – l’agenzia dell’Unione europea che si occupa della sicurezza delle reti –, aveva scartato qualsiasi ipotesi di accesso nascosto o laterale in una dichiarazione congiunta. La ragione è che le backdoor “aumenterebbero la superficie di attacco per abusi malevoli, e dunque avrebbero implicazioni ben maggiori per la società”.

Dunque quali ipotesi potrebbero restare? Forse la richiesta ai produttori di apparecchi e servizi di comunicazioni di limitare l’implementazione di default della crittografia forte? È la tesi avanzata da Nate Cardozo, legale della Electronic Frontier Foundation, storica associazione per i diritti digitali, in una presentazione al Defcon 2016, il noto raduno hacker di Las Vegas. “Il governo non è stupido”, ha dichiarato l’avvocato riferendosi agli Stati Uniti. “Sanno che non c’è un modo per togliere la crittografia forte dalle mani di chi sia determinato a usarla. Ma è invece possibile toglierla a chiunque entri in un negozio per comprare un iPhone”. O a chi scarichi una app.

“Piuttosto che indebolire per tutti la crittografia attraverso delle backdoor, le spie dovrebbero usare altri mezzi”, scriveva nel gennaio 2016 l’“Economist”. “Gli attacchi di novembre a Parigi sono potuti avvenire non perché i terroristi avessero chissà quali magiche capacità coi computer, ma perché le informazioni sulle loro attività non sono state condivise. Quando necessario, la Nsa e altre agenzie possono bucare i telefoni e i computer dei sospettati. È un’attività più difficile e lenta di una backdoor universale – ma è più sicura per tutti gli altri”.

Come vedremo nel prossimo capitolo, gli Stati hanno in realtà molti modi per raccogliere informazioni sulle persone, malgrado tutto. Ma per restare nell'ambito dell'antiterrorismo, vale la pena riportare anche quanto scritto da The Grugq, un esperto di sicurezza informatica noto a livello internazionale, che vende anche exploit e vulnerabilità ai governi (quindi non il tipico "attivista dei diritti digitali"): "Malgrado la retorica iperbolica sui pericoli delle 'app di messaggi cifrati' che creerebbero uno 'spazio sicuro per terroristi', la realtà non assomiglia alla propaganda. Anche le migliori app cifrate offrono solo una privacy limitata proteggendo il contenuto dei messaggi degli utenti. Le app di messaggistica per smartphone, incluse quelle cifrate end-to-end, producono diverse quantità di metadati – tra le grandi e le enormi quantità. L'analisi delle informazioni [sugli attentati terroristici in Francia] disponibili su fonti aperte suggerisce che i servizi di intelligence non stiano sfruttando appieno i vantaggi di avere a disposizione questi metadati".

I metadati sono le informazioni relative a una comunicazione. Nel caso di queste app, ricorda ancora The Grugq, corrispondono ai numeri di telefono che sono legati agli account; agli indirizzi Ip usati dal telefono per connettersi al proprio profilo, che a loro volta possono essere geolocalizzati e collegati alla compagnia di telecomunicazioni che li gestisce e dalla quale si possono ottenere ulteriori informazioni; al registro delle operazioni relative ai messaggi ("transaction log"), dove si trovano l'origine e la destinazione (quindi i numeri di telefono) dei messaggi scambiati; al numero di questi ultimi; alla loro dimensione nonché data e ora di invio; e ancora all'orario in cui il telefono era connesso e il profilo attivo. "Tutte queste informazioni, e probabilmente anche altre, sono disponibili sia per WhatsApp che per Telegram", scrive The Grugq, che fa anche un esempio concreto in cui il loro utilizzo sarebbe servito per individuare alcuni membri della cellula che ha organizzato gli attentati del novembre 2015 in Francia.

La terza direttrice su cui si sviluppa la narrazione su Isis e Rete è quella del cyber-terrorismo. Un termine che è già di per sé un concentrato di ambiguità, specie quando riferito al sedicente Stato islamico o in generale ai terroristi. Una espressione, scriveva già qualche anno fa un rapporto della società di sicurezza Symantec, che "sta diventando sempre più comune nella cultura popolare; e tuttavia ancora non si è consolidata una chiara

definizione di cosa significhi [...] Se chiedete a dieci persone che cosa è il cyber-terrorismo, avrete almeno nove risposte diverse!".

Ad aiutarci questa volta arriva l'Fbi, che fornisce una definizione farraginosa ma dettagliata. Secondo l'agenzia investigativa statunitense, il cyber-terrorismo è qualsiasi "attacco premeditato e motivato politicamente, contro informazioni, sistemi informatici, software e dati, che potrebbe produrre violenza contro obiettivi non militari da parte di gruppi non statali (subnazionali) o agenti clandestini". I suoi target saranno soprattutto installazioni militari, centrali elettriche e nucleari, sistemi di controllo del traffico aereo, dighe, e via dicendo.

Nel caso dell'Isis, i media usano la definizione di cyber-terrorismo anche per includere semplicemente il suo massiccio uso della Rete, perlopiù a fini propagandistici e di visibilità. Ma nella realtà si sta parlando di utilizzare Internet come canale di attacco diretto in grado di produrre danni consistenti a infrastrutture con ricadute violente sulle persone. E qui bisogna aprire una parentesi sul cyber-terrorismo in generale e su come viene citato spesso a sproposito.

"31.100 circa: il numero di articoli su riviste e giornali pubblicati fino ad ora per discutere il fenomeno del cyber-terrorismo. Zero: il numero di persone che sono state ferite o uccise dal cyber-terrorismo nel momento in cui questo articolo va in stampa". Così scriveva nel 2012 Peter W. Singer, uno degli analisti più brillanti sul tema, consulente della Difesa americana e fellow di vari centri di ricerca. Il suo articolo, *The Cyber Terror Bogeyman*, sebbene abbia ormai qualche anno, è ancora una delle letture più illuminanti al riguardo. La parola violenza è centrale in questa definizione, ricorda Singer, mentre molte discussioni imbottiscono l'espressione cyber-terrorismo con qualsiasi malefatta online.

Se però restiamo aderenti alla definizione più ristretta, ci rendiamo conto che il rischio di atti terroristici attraverso la Rete da parte dell'Isis o di suoi sostenitori sia, almeno per il momento, molto basso. "Far fuori dei generatori idroelettrici o progettare un malware come Stuxnet che danneggia delle centrifughe nucleari modificandone la velocità non richiede soltanto le capacità e gli strumenti per penetrare in un sistema informatico. Significa anche sapere cosa fare una volta che ci sei dentro. Procurare danni veri richiede una comprensione delle apparecchiature e di come funzionano, dell'ingegneria e della fisica sottostanti", scrive Singer.

Dunque, è la sua conclusione, coincidente con la valutazione di altri analisti come il professore dell'Accademia navale statunitense George R. Lucas, condurre un attacco di massa con mezzi informatici supera di gran lunga, per ora, le capacità intellettuali e organizzative di gruppi terroristici.

Peraltro, stando alla definizione più ristretta, anche il cyber-attacco più sofisticato ad oggi mai compiuto, Stuxnet, non rientrerebbe in quei parametri, configurandosi come un atto di sabotaggio che ha danneggiato lo sviluppo nucleare dell'Iran, ma senza avere ricadute dirette sulle persone (se si escludono gli scienziati iraniani uccisi per strada da sicari, ma questa è evidentemente una vicenda parallela, per quanto collegata).

Tornando dunque all'Isis, vediamo che almeno sul fronte digitale di terrorismo ne ha prodotto ben poco, anzi nulla, stando alla definizione dell'Fbi. Più in generale, fino al 2016, la maggioranza degli esperti ritiene che l'Isis e i suoi sostenitori abbiano scarse capacità di attacco informatico. E in un certo senso, dal loro punto di vista, averne o meno importa poco: per i jihadisti è molto più facile spargere terrore attraverso azioni fisiche; e la Rete è prima di tutto veicolo di propaganda (mentre la cassa di risonanza, più che i social, sono gli stessi media tradizionali).

Hacker pro-Isis

Una delle prime istanze di hacker pro-Califfato emerge nell'agosto 2014, a due mesi dalla proclamazione del sedicente Stato islamico in Iraq e Siria. Su Twitter compare il profilo @KhilafaHackers, ovvero Caliphate Hackers, i quali sostengono di aver mandato offline vari siti anti-islamici. Inoltre chiedono donazioni su un indirizzo bitcoin. Tuttavia, sebbene subito associati all'Isis dai media, precisano di "non lavorare per lo Stato islamico e di non essere nemmeno affiliati". Sebbene lo sostengano "fino a un certo punto", la loro agenda, per quanto si riesce a capire, è "supportare la lotta contro il governo centrale dell'Iraq". Per la cronaca, quell'indirizzo bitcoin ha ricevuto una sola donazione, nel maggio 2015, equivalente all'epoca a circa 98 euro.

Intanto, a un mese da questa prima tenue apparizione di hacker simpatizzanti dell'Isis, i media si scatenano. Nel settembre 2014 il "Daily Mail" e altri giornali scrivono che l'Isis sta creando una sorta di "cyber-Califfato" tutto protetto da cifratura (qualunque cosa questa espressione

significhi) per poter condurre attacchi informatici contro l'Occidente. La fonte sembra essere l'intelligence occidentale. Nel mirino ci sarebbero siti di governi, infrastrutture critiche, compagnie energetiche, banche e via dicendo.

Su almeno un dettaglio, comunque, il "Daily Mail" (e altri) sembrano essere abbastanza informati: quando rilevano il ruolo che potrebbe giocare Junaid Hussain, un hacker britannico di Birmingham, all'epoca (prima della sua trasformazione in jihadista) con contatti perfino in Anonymous, insomma proveniente dal mondo dell'hacktivismo[25] e infine arruolatosi in Siria nelle file dello Stato islamico, per poi rinascere online come Abu Hussain Al-Britani.

Apparentemente, tra gli attacchi prodotti dai primi e ancora misteriosi hacker pro-Califfato c'è la violazione dell'app mobile della testata iperlocale americana "Albuquerque Journal", su cui fanno comparire un articolo intitolato, in modo a dir poco puerile: "Natale non sarà più felice". L'immagine scelta dagli hacker contiene la sigla Cyber Caliphate, che a questo punto non si capisce se sia stata prima inventata dai media e poi abbracciata dagli attaccanti o viceversa. È presente anche la frase "I love you Isis", mentre la motivazione dichiarata dell'azione sono i bombardamenti americani contro l'Isis. Abbiamo tutti i vostri dati, millantano gli hacker, rivolgendosi ai residenti di quella regione.

La prima azione realmente degna di nota attribuita a questo gruppo sembra essere però l'hackeraggio del profilo Twitter di Centcom, il comando militare centrale statunitense, avvenuto nel gennaio 2015. Anche qui immagine e slogan simili, compresa la scritta "I love you Isis". Ovviamente l'azione, per quanto imbarazzante per il Pentagono, non è una Armageddon digitale. Come mi ha detto all'epoca James Lewis, esperto di cyber-sicurezza del Center for Strategic and International Studies, noto think tank di Washington: "L'incidente di Centcom, più che riflettere le capacità degli attaccanti, mostra l'assenza di capacità negli attaccati. Probabilmente il personale che gestisce gli account social del comando ha scelto delle pessime password. Certamente, con l'arrivo di una nuova generazione di jihadisti dall'Occidente, le capacità informatiche dei terroristi sono aumentate. Ma questi gruppi, incluso l'Isis, non sono davvero interessati ad hackerare infrastrutture critiche; il loro interesse verso la Rete è a fini di propaganda e reclutamento, ed è lì che

concentrano gli sforzi. Oppure nell'attacco di target semplici ma simbolici".

O, ancora, nel colpire attivisti nella loro area geografica d'influenza con malware rudimentali ma pericolosi qualora vadano a segno, perché in grado di rivelare l'identità di oppositori dello Stato islamico, con le prevedibili conseguenze. Uno scenario delineato, nel dicembre 2014, da un report del Citizen Lab, laboratorio dell'Università di Toronto dedito a dare la caccia ai malware usati da governi o altre entità contro dissidenti, giornalisti e organizzazioni scomode. A novembre di quell'anno i ricercatori hanno infatti trovato le tracce di un software malevolo, che era stato inviato via mail agli attivisti siriani anti-Isis che gestivano anonimamente il sito Raqqa is Being Slaughtered Silently (Rss), dove erano denunciate le violenze e gli orrori compiuti dai membri dello Stato islamico sulla popolazione locale di Raqqa, in Siria. Il programma, pur essendo uno strumento rudimentale, se veniva scaricato sotto forma di allegato alla mail riusciva a ottenere l'indirizzo Ip della vittima, e quindi a localizzarla.

Si trattava di uno strumento rozzo, non come quelli usati dagli hacker siriani pro-Assad del Syrian Electronic Army contro gli oppositori del regime. Questi hacker infatti colpivano attivisti per i diritti umani infettandoli con un vero e proprio "Rat", un software malevolo che poi prendeva il controllo del computer della vittima spiandone le attività. Il software usato contro il gruppo di Rss era invece meno sofisticato e si limitava a geolocalizzare i pc. Nondimeno, gli effetti potevano essere letali perché, una volta individuati, gli attivisti anti-Isis di Raqqa rischiavano la morte. Per il Citizen Lab è probabile che il malware fosse collegato proprio all'Isis.

Se delle potenzialità hacker dell'Isis sappiamo poco, e quel poco non impressiona, l'esistenza di una più ampia area di hacktivismo di natura islamista si svela nel gennaio 2015. Poco dopo gli attentati in Francia di quel mese, si sviluppa online un'ondata di attacchi informatici rivolti a siti francesi, nota come "OpFrance" ("operazione Francia"). L'apice si ha tra il 10 e il 16 gennaio, per un totale di circa 1300 target colpiti, siti mandati offline o defacciati, mi conferma l'Agenzia nazionale per la sicurezza dei sistemi informativi. Non sono pochi, ma molto meno della cifra di 19mila siti che circola inizialmente sui media. Inoltre si tratta di siti minori, scelti a

caso in base alle loro vulnerabilità, setacciate attraverso programmi appositi che cercano falle nei "plug-in" (non aggiornati) dei principali sistemi per pubblicare siti web, i cosiddetti Cms (Content management systems), come Wordpress, Drupal o Joomla.

A muoversi è una rete informale di squadre e singoli composta da una ventina di entità, almeno sulla base di una mia ricognizione dell'epoca. Tra queste, gli AnonGhost, degli hacktivisti alla Anonymous concentrati soprattutto sulla causa palestinese, e il loro fondatore Mauritania Attacker. O loro sigle collegate come gli Al-Aqsa. O il Fallaga Team, un gruppo tunisino e anti-israeliano. E ancora, gli Izzah Hackers, anche loro fortemente pro-Palestina e in passato impegnati in operazioni come "Op Save Gaza" ("operazione Salva Gaza"). E poi gruppi che sembrano sposare una agenda islamista molto più netta, come il Middle East Cyber Army e la United Islamic Cyber Force.

La loro posizione ideologica è espressa bene da un commento che nel gennaio 2015 mi ha rilasciato via Twitter l'amministratore dell'account United Islamic Cyber Force: "'OpFrance' nasce per vendetta per come gli infedeli ('kuffar') si comportano con i musulmani e con l'Islam". Mi colpisce il fatto che, pur dicendomi di non avere connessioni con l'Isis, arrivi a giustificare le uccisioni di chi insulta il Profeta. Nondimeno, gran parte di queste sigle sembrano appartenere ad attivisti islamici – o in alcuni casi islamisti – che tuttavia restano ancora ben lontani dall'estremismo dell'Isis. "Sono musulmano ma rispetto tutte le religioni", dichiarava nel 2014 Mauritania Attacker.

Certo, non si può escludere col tempo un loro processo di radicalizzazione. Che però, diversamente dalla vulgata corrente, è probabile che avvenga offline. Ne abbiamo almeno un esempio illustre: Junaid Hussain, il quale finché stava solo online era un hacktivista britannico di area musulmana in contatto con hacker e membri di Anonymous di tutti i credi, inclusi atei e anarchici; e che dopo essere stato in prigione è riemerso come foreign fighter. Hussain è probabilmente l'artefice dell'attività di hacking ascrivibile allo Stato islamico tra l'agosto del 2014 e l'agosto del 2015. La nascita e lo sviluppo del Cyber Caliphate sono attribuiti a lui; e per lo stesso motivo, con la sua scomparsa nell'estate 2015, anche il potenziale cyber-offensivo del Califfato ne è uscito ridimensionato.

Hussain è un adolescente di Birmingham di origine pachistana che già a 11 anni inizia a dedicarsi all'hacking; a 15, con un amico, forma una "crew" di nome Team Poison. "Sono diventato politicizzato guardando video di bambini ammazzati in Paesi come il Kashmir e la Palestina", dice Hussain in una intervista al sito Softpedia. Da leader di Team Poison il giovane – che online adotta lo pseudonimo di Trick – hackera carte di credito israeliane in una operazione pro-Palestina; ma soprattutto prende di mira la linea telefonica antiterrorismo dell'intelligence britannica, bombardandola di chiamate-scherzo; e diffonde la rubrica dell'assistente di Tony Blair. Entra in contatto con gruppi e attivisti di Anonymous, con alcuni dei quali condivide ad esempio la causa palestinese.

Trick viene però individuato e nel settembre 2012 è condannato a sei mesi di prigione. Dopo i quali apparentemente sparisce, offline e online. Riemergerà solo nell'agosto 2014, tra le fila dello Stato islamico, dopo aver raggiunto la Siria, non si sa ancora come e quando. Qui inizierà a coordinare le azioni digitali del Califfato, adottando il nome Abu Hussain Al-Britani nel suo profilo Twitter, che verrà chiuso decine di volte – e che lui riaprirà cambiando solo il numero alla fine del nome. In Siria, si sposerà anche con una britannica di 45 anni, una bionda ex punk rocker convertita all'Islam ma soprattutto allo Stato islamico, Sally Jones.

La popolarità online di Hussain e le sue competenze di hacking rispetto ad altri jihadisti lo fanno finire presto nella lista americana degli obiettivi da eliminare. E così accadrà: Hussain verrà ucciso nell'agosto 2015, dopo appena un anno di Califfato (e di cyber-Califfato, che come abbiamo visto inizia proprio in contemporanea all'arrivo del giovane), attraverso l'attacco di un drone nei pressi di Raqqa. Aveva 21 anni. Secondo il "Times", Hussain sarebbe stato tradito da un link inviatogli attraverso Surespot, una app di messaggi cifrati, da una spia del Gchq, l'intelligence britannica specializzata in comunicazioni elettroniche. Cliccando sul link il capo del Cyber Caliphate avrebbe rivelato la sua geolocalizzazione. La stessa idea – anche se l'esecuzione era più sofisticata – utilizzata dall'Isis contro gli attivisti di Raqqa.

Il cyber-Califfato finisce con Hussain. Anche se dopo qualche mese, a fine novembre, riemergerà improvvisamente nelle vesti di una nuova formazione, gli Islamic State Hackers, una sorta di federazione di varie entità e gruppi guidata da alcuni profili Twitter che si fanno chiamare Isis

Lion, Dr. Isis, ENG ISIS, ecc. E che iniziano a pubblicare indirizzi e numeri di telefono di personale militare americano. Lo faranno altre volte in futuro, sebbene molti di questi dati sembrino vecchi o recuperati da precedenti hack, o ricavati semplicemente da fonti aperte. Poi il gruppo pubblica link a guide di sicurezza informatica e di hacking. O riferimenti a Isdarat, uno dei pochissimi siti web di area Isis presenti nel Dark Web.

Malgrado i toni roboanti e minacciosi, il sequestro di simboli, le modalità dell'hacktivismo alla Anonymous, e i tutorial di informatica, l'impressione è di non essere affatto di fronte a un team di hacker particolarmente pericoloso. Il fronte più attivista e frammentato di questi hacktivisti pro-Isis si riunirà poi, nell'aprile 2016, in un collettivo dal nome United Cyber Caliphate. Ma secondo un report pubblicato poco dopo dalla società di analisi Flashpoint e intitolato *Hacking for ISIS*, questa armata un po' brancaleone, così come le altre o precedenti entità di hacker pro-Isis, non opera in maniera ufficiale; non mostra capacità di attacco avanzate o dirette verso target sofisticati; e, alla fine, sembra essere poco organizzata e finanziata.

In questo quadro, c'è però almeno un'azione attribuita al Cyber Caliphate che è stata piuttosto importante. E che si è conclusa con un giallo. Nell'aprile 2015, un attacco informatico mette KO il network televisivo francese Tv5Monde, mandando fuori uso non solo il suo sito e i suoi profili social, ma soprattutto le sue trasmissioni. Che subiscono un blackout per 18 ore, e ancora per giorni a seguire non torneranno a una situazione normale. In pratica gli hacker riescono ad avere il controllo della rete televisiva fondata dal governo francese nel 1984, sabotando simultaneamente 11 suoi canali.

L'attacco viene rivendicato dal Cyber Caliphate, che pochi mesi prima, come abbiamo visto, si era impossessato del profilo Twitter di Centcom – e poco dopo anche di quello della rivista "Newsweek". Ma qui è un'altra faccenda; è una rete tv nazionale (che trasmette in tutto il mondo) ad essere bloccata e danneggiata. Durante l'episodio, gli hacker pubblicano anche, sulla pagina Facebook della stessa tv, le carte d'identità di alcuni soldati francesi che sarebbero coinvolti in operazioni anti-Isis, oltre a minacce contro gli stessi. I procuratori di Parigi aprono un'inchiesta per terrorismo. Si mobilita il governo. Il primo ministro Manuel Valls definisce l'attacco "un insulto inaccettabile alla libertà di informazione ed espressione". Per il

direttore generale della tv, Yves Bigot, i loro sistemi hanno subìto danni pesanti; e l'attacco deve essere stato preparato per settimane. È decisamente un salto di qualità per il Cyber Caliphate.

Ma passano pochi mesi e, nel luglio dello stesso anno, arriva un colpo di scena. Un'analisi della società di sicurezza americana FireEye sostiene che a perpetrare l'attacco sarebbero stati hacker russi che fingevano di essere il Cyber Caliphate. E non hacker russi qualsiasi, ma membri del gruppo Apt28, noto anche come Sofacy, Sednit, Fancy Bear, gruppo che abbiamo già incontrato nel primo capitolo. Che quindi avrebbe usato l'etichetta del Cyber Caliphate come una copertura. I ricercatori di FireEye arrivano a questa conclusione analizzando l'infrastruttura utilizzata dagli attaccanti, che ha vari punti in comune con quella di Apt28[26]. "La Russia ha una lunga storia di utilizzo di operazioni di disinformazione per accrescere la confusione a proprio beneficio" commenta su Buzzfeed uno degli analisti di FireEye, Jen Weedon. "In questo caso, è possibile che il Cyber Caliphate dell'Isis potesse essere una distrazione. E questo attacco poteva essere un test per vedere se si poteva lanciare un attacco coordinato su un media in grado di bloccarne le trasmissioni". Una conclusione, quella della pista russa, a cui arriva in contemporanea anche una indagine della rivista francese "L'Express".

Dunque l'attacco a Tv5Monde è stato realizzato da spie russe che hanno usato la bandiera del Cyber Caliphate per nascondersi? Quasi un anno dopo, c'è chi arriva a sostenere perfino che l'intero Cyber Caliphate, e quindi non solo quello specifico attacco, sia una cosiddetta "false flag": una operazione di intelligence in cui ci si finge un altro soggetto. Dunque tutta l'attività del cyber-Califfato sarebbe spuria, finta, una invenzione di Mosca. A dare credito a questa versione è un articolo di "Der Spiegel" del giugno 2016, che però a sua volta riporta fonti anonime dell'intelligence tedesca. Ma è davvero immaginabile che tutta l'operazione sia una montatura? E che dire di Junaid Hussain?

In realtà, non sono mai state mostrate prove del cyber-Califfato come false flag. E incolpare i russi nel caso specifico, e nel mezzo di forti tensioni sul terreno digitale tra Mosca e Washington, poteva far comodo a molti. Resta però l'interrogativo almeno su Tv5Monde. Qui gli scenari possono essere diversi, e li aveva delineati Trend Micro in un articolo online: il fatto che siano state trovate tracce di Apt28 sulla stessa infrastruttura

potrebbe semplicemente significare che anche i russi, come il Cyber Caliphate, avevano compromesso Tv5Monde; o che per primi sono entrati i russi, e poi per qualche motivo hanno passato i dati, direttamente o indirettamente, agli hacktivisti islamici che comunque all'epoca, sotto la guida di Hussain, erano probabilmente all'apice delle proprie capacità; o infine che la responsabilità sia stata interamente e soltanto dei russi (fingendosi Cyber Caliphate).

Quest'ultima tesi, però, non convince tutti. "Non ci sarebbero molte prove tecniche per attribuire l'attacco contro Tv5Monde ad Apt28 o Sofacy", mi ha detto Vicente Diaz, analista di Kaspersky. "Inoltre il tipo di attacco non sarebbe in linea con il modo di operare del gruppo, che è dedito al cyber-spionaggio e quindi preferisce mantenere un basso profilo". Come al solito, l'attribuzione resta un terreno scivoloso.

Tuttavia, se il Cyber Caliphate era usato anche solo in parte dai russi per operazioni di guerra psicologica e di disinformazione, tale copertura è stata fatta saltare, dall'intelligence occidentale, nel giugno 2016. Proprio quando stava per innescarsi una spirale sempre più stretta di tensioni sul fronte digitale tra Russia e Stati Uniti, con l'hackeraggio delle mail e dei documenti del Comitato nazionale del Partito democratico americano. Alla luce dell'estate 2016, un Cyber Caliphate in salsa russa, anche solo per alcune operazioni, acquista improvvisamente più senso di quanto non lo avrebbe normalmente. E mostra quanto sia difficile muoversi, anche giornalisticamente, su un terreno così instabile.

Per concludere, vorrei riprendere quanto diceva il già citato Peter W. Singer: "Non è che il cyber-terrorismo, e in particolare gli attacchi a infrastrutture critiche, non destino preoccupazione. Ma fino ad ora, quello che i terroristi hanno ottenuto in Rete non raggiunge le nostre paure, i loro sogni o anche quello che sono riusciti a fare con mezzi tradizionali. [...] E quello che i gruppi terroristici apprezzano di Internet è esattamente ciò che apprezziamo noi – un servizio affidabile, sistemi di pagamento, anonimato virtuale, ecc. –, il che complica il nostro vecchio modo di pensare alle minacce. E ciò significa che, quando affrontiamo il terrorismo, così come in altre aree della cyber-sicurezza, dobbiamo essere consapevoli delle nostre abitudini, di come usiamo la Rete e di come attori malevoli potrebbero approfittarsene".

[23] http://www.csmonitor.com/World/Global-News/2016/0710/Why-has-pro-ISIS-Twitter-traffic-dropped-45-percent-in-two-years.

[24] https://www.lawfareblog.com/stop-isis-recruitment-focus-offline.

[25] Da "hack" e "attivismo", ovvero l'uso di mezzi informatici per veicolare messaggi politici. Un esempio tipico è il movimento di Anonymous.

[26] Ad esempio, il sito usato dal Cyber Caliphate per pubblicare i dati sull'hack di Tv5Monde è ospitato (hostato) sullo stesso blocco di indirizzi Ip usato anche dai russi; lo stesso vale per il server e il "registrar", un'azienda che rivende l'assegnazione dei nomi a dominio e altri servizi internet.

7.
Frontiere della sorveglianza

È una calda sera di luglio a Roma. Meno calda che a Dubai, da dove Simone Margaritelli (noto online come evilsocket) è appena rientrato dopo un viaggio per valutare una proposta di lavoro.

Simone ha 31 anni, si è avvicinato da giovane ai computer e all'hacking, ha imparato molte cose da autodidatta, "ha fatto danni" – per usare la sua espressione – finché a un certo punto ha deciso di dedicarsi a qualcosa di più costruttivo. Ora è un noto ricercatore internazionale. Vive in Italia ma lavora per Zimperium, azienda di San Francisco che opera nella sicurezza difensiva per dispositivi mobili. Ma in passato ha lavorato molto anche in quella che si definisce "sicurezza offensiva". In particolare ha sviluppato BetterCap, un noto strumento "open source" per condurre degli attacchi sul traffico online di un utente e spiarlo, anche qualora il suo traffico sia cifrato.

Simone dopo qualche giorno deve imbarcarsi di nuovo su un aereo e volare a Las Vegas, dove si sta per tenere l'edizione 2016 di Defcon, uno dei più importanti raduni hacker globali. Prima però vuole finire di scrivere un articolo in inglese per il suo sito. Lo pubblica nella serata del 27 luglio e il titolo non è di quelli che passano inosservati: "Come l'intelligence degli Emirati Arabi Uniti ha cercato di assumermi per spiare sulla popolazione".

Qui il ricercatore racconta di essere stato contattato a inizio luglio da un italiano che vive negli Emirati, legato a una grossa società di origine israeliana specializzata in tecnologie di intercettazione. L'uomo gli propone un lavoro a Dubai, in un progetto inizialmente fumoso ma che si rivela poi essere la creazione di una task force di ricerca e sviluppo di soluzioni di

sorveglianza su larga scala. Il committente sembra essere il governo degli Emirati. Simone, sebbene già insospettito dai primi termini dell'offerta, decide di approfondire la questione e vola nel Paese del Golfo a fine luglio. "Avevo già deciso di rifiutare il lavoro dall'inizio, ma ho approfittato della vacanza a Dubai, se non altro per capire cosa stavano combinando".

Qui, in un incontro all'hotel Marina Plaza, nel quartiere di Dubai Marina, definito "una spiaggia tra grattacieli", ottiene nuovi dettagli: il progetto vuole sviluppare e implementare una serie di soluzioni per intercettare su larga scala il traffico Internet, diffondendo delle sonde in luoghi pubblici come aeroporti e centri commerciali. Come? Me lo spiega in quei giorni Margaritelli: "Quando ho chiesto chiarimenti su cosa fossero esattamente queste sonde, mi è stato risposto (e poi ho verificato di persona) che in ogni mall, ogni ristorante, ogni bar, ogni palazzo, ogni hotel, insomma ogni singolo posto dove c'è connessione, il governo ha messo queste simpatiche scatoline il cui unico scopo è quello di tracciare e catturare dati 24 ore su 24 su chiunque (non ci sono intercettazioni selettive come da noi, quando ho scritto chiunque intendo letteralmente chiunque). Oltre alle intercettazioni passive su reti 2G, 3G, 4G [quindi su tutte le reti mobili] e su tutta la rete fissa (con l'accordo degli operatori) sono anche previste delle capacità per fare attivamente 'exploiting', ovvero per infettare gli apparecchi nella zona". E la zona includerebbe almeno Dubai e Abu Dhabi.

"L'obiettivo del governo, quindi il nostro, è di prendere il controllo di ogni dispositivo elettronico a portata d'azione", spiega a Margaritelli uno dei suoi contatti negli Emirati. E prosegue: "Immagina che ci sia una persona di interesse nel centro commerciale di Dubai. E che abbiamo già piazzato tutte le nostre sonde nella città: schiacciamo un pulsante e... Boom! Tutti gli apparecchi nel centro commerciale sono infettati e tracciabili".

Ma come funziona questo sistema di sonde? E cosa è in grado di vedere? "Fondamentalmente si tratta di diverse 'scatole' hardware distribuite su tutto il territorio per effettuare attacchi 'man-in-the-middle' su ogni dispositivo connesso", mi dice Margaritelli.

Un attacco man-in-the-middle (l'uomo in mezzo, spesso abbreviato come Mitm) consiste nell'inserirsi in mezzo a una conversazione o a un flusso di dati fra due parti. Ad esempio nel traffico tra un "client" e un

server[27], come quello che avviene ogni volta che col nostro computer ci colleghiamo a un sito. Una volta inserito nel flusso, l'attaccante può vedere i dati che sono scambiati (intercettare), ma può anche modificare una parte degli stessi. "Questi apparecchi sono installati nei nodi principali delle compagnie telefoniche; oppure sono dei finti punti di accesso Wi-Fi in luoghi pubblici; o stazioni base per la telefonia mobile", prosegue Margaritelli. "Attraverso simili dispositivi ci si interpone nel traffico e a quel punto si possono anche compiere veri e propri attacchi informatici, infettando i dispositivi con malware specifici".

In teoria il traffico cifrato, quello che per esempio usiamo per collegarci ai siti che implementano il protocollo https[28] – come Gmail, Facebook, e l'internet banking –, è più difficile da intercettare in questo modo, perché i dati sono illeggibili. Ma se l'attaccante controlla un punto d'accesso a Internet di un utente potrebbe reindirizzarlo verso un sito fasullo e provare a ingannarlo in questo modo. Una persona smaliziata probabilmente si accorgerebbe della manipolazione, perché il sito mascherato non sarebbe perfettamente identico all'originale, o non avrebbe più l'https. E tuttavia esiste un metodo ancora più sofisticato per ingannare gli utenti: è il caso in cui un attaccante, ad esempio un governo, ottenga dei certificati digitali "falsi", cioè quegli strumenti usati dai siti web per garantire la propria autenticità e quella del canale di comunicazione cifrato.

I certificati li vediamo ogni volta che clicchiamo sul lucchetto all'inizio di un indirizzo https e garantiscono che la nostra connessione a siti come Facebook sia protetta, e che quel sito sia veramente Facebook o chi dice di essere. I certificati sono rilasciati da una serie di organizzazioni private (ma in alcuni casi legate ai governi) che fanno un po' da notai e che sono chiamate Autorità di certificazione (Certificate Authority). La maggior parte dei browser e dei sistemi operativi hanno un proprio set di certificati rilasciati da diverse Autorità attraverso i quali verificano, sempre grazie alla crittografia, l'autenticità di un sito a cui ci stiamo connettendo con il protocollo https (quindi in modo cifrato e protetto). Ma se una di queste organizzazioni rilascia a una terza parte un certificato finto dove si mostra che sei Facebook anche se non lo sei, chi lo utilizza è in grado di ingannare gli utenti che provino a connettersi al social network, facendoli collegare invece a un proprio sito identico a Facebook e con tanto di https iniziale, per poi intercettarne il traffico (e infine ridirigerli sul vero Facebook).

Ora, dopo questo *excursus* sui certificati, dovrebbe essere più chiaro come sia possibile realizzare attacchi man-in-the-middle anche su un traffico cifrato e quindi teoricamente blindato. "Per quanto riguarda il traffico cifrato – quello ssl/https – la persona che mi ha contattato mi ha spiegato che il governo avrebbe una propria Autorità di certificazione e che quindi in molti casi sono in grado di intercettare anche quel traffico", aggiunge Margaritelli.

L'unica cosa che rimarrebbe fuori da un simile sistema di "ascolto" è il traffico protetto da crittografia end-to-end, perché la cifratura e la decifratura avvengono direttamente nel dispositivo di partenza (il mio smartphone) e in quello di arrivo (quello della mia amica), e non quando il mio client contatta il server di Facebook.

"Queste persone cercano di attirare giovani talenti della sicurezza informatica promettendo cospicue somme di denaro, vari bonus, appartamenti e, soprattutto, presentando un ambiente di lavoro stimolante intellettualmente e professionalmente", scrive nel suo sito Margaritelli, il quale ha rifiutato un'offerta che prevedeva uno stipendio da 13-17mila euro al mese. "Ma per quel che mi riguarda, la libertà di espressione è indiscutibile".

Il progetto degli Emirati Arabi Uniti

Dopo aver pubblicato l'articolo, Margaritelli mi dice di essere stato raggiunto da numerosi ricercatori e giornalisti che volevano saperne di più o che avevano esperienze da condividere. Gli chiedo quali sono i principi etici che segue in questi frangenti per accettare un lavoro, specie se si tratta di sicurezza offensiva. "Sono tre", mi risponde. "Conosci sempre l'utilizzatore finale del tuo sistema. Conosci il tuo target e rifiuta operazioni su larga scala. E non aiutare Paesi in cui non vige la libertà di parola, di stampa o in generale nei quali le opinioni scomode vengono represse con la violenza".

Gli Emirati Arabi Uniti sono una federazione retta da sceicchi, in pratica composta da monarchie ereditarie assolute. Gli Emirati sono sette, i due principali sono quelli di Abu Dhabi e Dubai. Esistono delle elezioni per un Parlamento solo consultivo, ma sono a suffragio limitato. La loro economia è basata sul petrolio e sul turismo (e sullo sfruttamento di manodopera

immigrata), ma negli ultimi anni Abu Dhabi e Dubai sono diventati un luogo accogliente anche per le aziende tech occidentali, soprattutto quelle del mondo della sorveglianza. È proprio a Dubai che si tiene ogni anno l'edizione regionale dell'Iss, la fiera più importante dell'industria delle intercettazioni delle comunicazioni e dell'intelligence, luogo di ritrovo da un lato delle forze dell'ordine e dei servizi segreti della regione mediorientale, dall'altro delle imprese occidentali della sorveglianza. Ma al di là di questa veste tecnologica – e di un'urbanistica aggressiva e mozzafiato, fatta di grattacieli futuristici, spiagge artificiali, spa, ristoranti, centri commerciali – c'è un cuore autocratico.

"Dietro una facciata sfarzosa e scintillante, gli Emirati Arabi Uniti nascondono la natura repressiva delle proprie istituzioni nei confronti di attivisti che è sufficiente postino un tweet critico per finire nei guai", scriveva nel 2014 Amnesty International, aggiungendo che il clima di paura durava dal 2011. "Il dissenso viene regolarmente colpito con persecuzioni, arresti, condanne, sparizioni forzate e in alcuni casi torture". Di farseschi processi di massa contro i dissidenti che chiedono alcune riforme scriveva già la Bbc nel 2013. E della persecuzione di attivisti parlava anche l'organizzazione per i diritti umani Human Rights Watch nel 2012. Nel 2015 l'organizzazione Freedom House classificava il Paese come "non libero", sottolineando che continuava a sopprimere il dissenso.

Soprattutto, gli Emirati sembrano avere una passione per le tecnologie di controllo della popolazione. Già nel 2010 annunciavano di voler sospendere i servizi di mail e messaggistica dei telefonini BlackBerry perché non riuscivano a monitorarli. E nel 2011 la federazione di Emirati iniziava a gettare le basi per un ampio progetto di sorveglianza, una serie di soluzioni che dovevano includere diversi tipi di sensori in un unico sistema di controllo. Nome in codice del progetto: "Falcon Eye".

Proprio nel luglio 2016 arriva il lancio ufficiale di tale sistema di sorveglianza da parte delle autorità di Abu Dhabi, benché si sappiano pochissimi dettagli, a parte il fatto che dovrebbe utilizzare anche videocamere di sorveglianza. A darne qualcuno in più è Rori Donaghy, un giornalista residente a Londra che scrive per la testata online "Middle East Eye" e che ha fondato un'organizzazione per monitorare gli abusi dei diritti umani negli Emirati, l'Emirates Center for Human Rights.

Il progetto – scrive il reporter – prevede di raccogliere un'ampia quantità

di dati sui movimenti e sulle attività delle persone utilizzando diverse tecnologie di sorveglianza, dalle videocamere in strada agli apparecchi smart connessi a Internet. Da tempo Donaghy studia con attenzione questo sistema e già a fine 2014 aveva scritto del coinvolgimento di una società israeliana. Che però manteneva un profilo molto basso, utilizzando jet privati per raggiungere Abu Dhabi da Tel Aviv: del resto, gli Emirati non riconoscono Israele come uno Stato e i due Paesi non hanno ufficialmente relazioni economiche o diplomatiche.

Tra l'altro, la stessa storia personale di Donaghy ha svelato ulteriori sistemi di sorveglianza. A forza di occuparsi di questi argomenti, lui stesso è diventato un target di ciò che denunciava. Nel novembre 2015 il giornalista riceve, infatti, una mail che ha come mittente una misteriosa organizzazione pro-diritti umani. La mail veicola in realtà uno spyware, un software spia che una volta installato potrebbe monitorare tutta l'attività del computer della sua vittima.

Donaghy però capisce che qualcosa non va, anche perché non è il primo attivista del Paese ad aver ricevuto un attacco del genere, come vedremo. E gira tutto al ricercatore di sicurezza Bill Marczak, che ha firmato vari rapporti di Citizen Lab, il laboratorio sulla sorveglianza dell'Università di Toronto, particolarmente specializzato in spyware usati dai governi. Così nel maggio 2016 esce un report del laboratorio canadese, che descrive una sofisticata campagna di spionaggio di matrice governativa ai danni di giornalisti e attivisti degli Emirati; e la chiama non a caso "Stealth Falcon".

Il Citizen Lab ha individuato almeno altri 24 cittadini del Paese presi di mira dallo stesso spyware, inviato anche via Twitter con un link; almeno tre di questi sono stati arrestati poco dopo averlo ricevuto; un altro è stato condannato in contumacia per aver insultato i governanti. Gli attacchi vanno avanti dal 2012 e mostrano uno spyware "fatto in casa", abbastanza sofisticato e che, secondo i ricercatori, mostrerebbe un avanzamento delle capacità tecnologiche degli Emirati. I quali avrebbero già usato spyware in passato, sempre stando a precedenti report di Citizen Lab, ma comprandoli da aziende occidentali come FinFisher, Hacking Team e Nso, società che vendono legalmente questi prodotti solo ad agenzie governative che dovrebbero usarli per indagare su criminali e terroristi.

La storia più incredibile avvenuta negli Emirati resta però un'altra.

L'attivista da un milione di dollari (e tre zero-day)

È il 10 agosto 2016. Ahmed Mansoor, che vive ad Ajmad, città non lontana da Dubai, e che da anni ormai non può più lasciare il Paese, riceve un sms sul suo iPhone. "Nuovi segreti sulle torture nelle prigioni statali", dice il messaggio, seguito da un link. Il numero di telefono da cui sembra provenire non è quello da cui arriva realmente. L'11 agosto sul telefono arriva un altro sms, molto simile, ma apparentemente da un diverso mittente. Mansoor, che da attivista dei diritti umani potrebbe essere tentato di cliccare sui link, se ne guarda bene. E a ragione. Già una volta è stato infettato da software malevoli, è scampato ad altri, ha ricevuto diversi e molteplici attacchi informatici o tentativi di intrusione.

"Quando l'ho visto, ho subito avuto dei sospetti perché il contenuto, tipicamente, era fatto per allarmare e spingere a cliccare. Inoltre in passato sono stato preso di mira molte volte dalle autorità e ora tendo a essere molto più cauto della media", mi dice al telefono. Così, forte della sua esperienza, gira i messaggi ai ricercatori di Citizen Lab. Questi, insieme a un'altra società di cyber-sicurezza, Lookout Security, analizzano i link, scoprendo che portano a una catena di tre exploit zero-days per iPhone, cioè a una concatenazione di tre codici di attacco sofisticati e pregiati perché, come abbiamo visto in precedenza, sfruttano vulnerabilità del software che sono ancora sconosciute se non agli attaccanti. I ricercatori hanno quindi avvisato Apple e, quando l'azienda ha chiuso le tre vulnerabilità con un aggiornamento a fine agosto per tutti gli iPhone, hanno pubblicato un report su quanto avevano scoperto.

Il trio di attacchi – soprannominato Trident dai ricercatori –, se attivato cliccando sul link degli sms, avrebbe fatto un jailbreak da remoto dell'iPhone 6 di Mansoor, installando uno spyware per sorvegliare tutta l'attività dell'uomo, dalle telefonate WhatsApp e Viber alle chat, alle mail, dall'accensione nascosta del microfono e della videocamera del dispositivo fino alla sua geolocalizzazione. Era la prima volta che un attacco di questo tipo, con jailbreak da remoto su un iPhone, veniva scoperto nel mondo reale come parte di una campagna mirata. Il jailbreak è una procedura che aggira i sistemi di sicurezza di un dispositivo Apple. Possono compierla gli utenti che vogliano installare app non approvate dalla casa madre, ma il contraltare è che il loro telefono diventa più vulnerabile. Gli iPhone sono

considerati tra gli smartphone più sicuri, ed è molto difficile infettarli da remoto se non sono stati sottoposti in precedenza a tale trattamento dai loro possessori. Un attacco in grado di violare un iPhone, facendo addirittura un suo jailbreak a distanza, è considerato molto raro. E anche molto costoso.

I ricercatori di Citizen Lab hanno analizzato il malware che avrebbe dovuto infettare e spiare il telefono di Mansoor, e hanno tracciato l'infrastruttura di server su cui si appoggiava per inviare di nascosto i dati rubati agli attaccanti. Secondo il rapporto pubblicato, si tratterebbe di un software spia di nome Pegasus, sviluppato da Nso Group, un'azienda di origine israeliana acquisita nel 2014 da una società di "private equity" americana e valutata quasi un miliardo di dollari. La portata e il costo dell'attacco, il tipo di vittima e il presunto coinvolgimento di Nso – che non ha mai confermato, tranne il fatto di vendere i suoi prodotti solo a Stati per le loro indagini – fanno pensare ai ricercatori che dietro l'azione ci possa essere il governo degli Emirati Arabi Uniti.

Ahmed Mansoor è un ingegnere e blogger di 45 anni, che da tempo cerca di far avanzare democrazia e stato di diritto negli Emirati, tanto che nell'ottobre 2015 ha ricevuto un importante premio da Amnesty International come difensore dei diritti umani. Ma nell'estate 2016, dopo il tentato attacco, diventa anche l'attivista più bersagliato da spyware che si conosca. Quello ricevuto via sms era almeno il terzo ricevuto negli ultimi anni. Non solo: i tre software spia che gli sono arrivati nel corso del tempo sarebbero stati prodotti da altrettante diverse società occidentali, che avrebbero avuto il governo degli Emirati Arabi Uniti (o alcune sue agenzie) come cliente.

Il primo spyware Mansoor lo riceve nel marzo 2011, attraverso una mail con allegato un finto pdf che i ricercatori di Citizen Lab successivamente riterranno essere stato sviluppato dall'azienda anglotedesca Gamma/FinFisher (che vendeva spyware ai governi, ma non ha mai confermato l'attribuzione). Poco dopo, l'uomo viene imprigionato insieme ad altri attivisti per aver insultato i governanti e poi "perdonato" nel novembre 2011 grazie a una campagna internazionale.

Nel luglio 2012 è la volta di un altro spyware – questa volta ricevuto attraverso un documento Word. Mansoor però capisce che qualcosa non va e contatta il Citizen Lab. "Quando sono entrato nel mio indirizzo mail

da un computer diverso, ho notato l'attività da un indirizzo Ip che non mi apparteneva", mi ha detto Mansoor. Attraverso quel software qualcuno si era scaricato tutta la sua posta di Gmail. I ricercatori dell'Università di Toronto pubblicano un report sul caso in cui scrivono che il tipo di software potrebbe essere stato prodotto dall'azienda italiana Hacking Team (che non ha mai confermato; anch'essa comunque ha sempre dichiarato di vendere i suoi software solo ai governi).

Ad ogni modo, è chiaro che qualcuno negli Emirati vuole controllare e intimidire l'attivista. Infatti, poco tempo dopo questo episodio, l'uomo viene aggredito fisicamente per strada per due volte. Oggi vive ancora negli Emirati e non può lasciare il Paese, malgrado le pressioni delle associazioni internazionali in suo favore.

Ma con il malware che gli è stato inviato via sms nell'estate 2016, Mansoor arriva a fare l'en plein di diversi tipi di spyware. Soprattutto, l'ultimo ricevuto ha una modalità di infezione molto più sofisticata. I tre zero-days per iPhone sono considerati dai ricercatori molto dispendiosi. Un attacco simile a quello, solo qualche mese prima, era valutato sul mercato delle vulnerabilità intorno a un milione di dollari, come abbiamo visto in un capitolo precedente. Mansoor diventa così ufficialmente "il dissidente da un milione di dollari". Nonché lo sconosciuto attivista degli Emirati, probabilmente attaccato dal suo stesso governo, che ha innescato suo malgrado un importante aggiornamento di sicurezza sugli iPhone di tutto il mondo, in una amara declinazione tech dell'effetto farfalla.

La rivelazione di zero-days per un sistema robusto come iOS di Apple segna una nuova stagione di hacking di apparecchi mobili. "Vedere non solo tre vulnerabilità, ma tre zero-days concatenati assieme per ottenere un jailbreak dell'iPhone con un clic, non ha precedenti. È infine arrivata l'era di attaccanti con molte risorse in grado di colpire degli smartphone invece di infrastrutture di rete o desktop", ha dichiarato Mike Murray, vicepresidente della società Lookout, alla testata specializzata "TechCrunch".

In questo quadro assumono una luce particolarmente sinistra una serie di nuove leggi sui crimini informatici, approvate dal presidente degli Emirati proprio nei giorni in cui Margaritelli pubblicava il suo resoconto del viaggio a Dubai. E che tra le altre cose puniscono – con multa e prigione – chiunque utilizzi una Vpn, una "rete privata virtuale", per proteggere il

proprio traffico Internet da sguardi indiscreti. Le Vpn stabiliscono un collegamento cifrato tra un utente e il fornitore del servizio, attraverso il quale passa poi tutto il traffico dello stesso utente. Questo permette a chi le utilizza di proteggere la privacy delle proprie attività online e anche di aggirare filtri e blocchi di siti web adottati da un governo attraverso i fornitori di servizi Internet, o Isp. Se un contenuto non è disponibile in una certa regione geografica perché bloccato, una Vpn correttamente configurata consente di aggirare quell'ostacolo. Nel caso in cui uno Stato censuri Twitter, un cittadino che si trovi in quella zona potrà comunque accedere al social network collegandosi prima a una Vpn che ha i server in un altro Paese.

Secondo la legge degli Emirati, è punibile chiunque usi una Vpn per accedere a un servizio vietato dallo Stato. Difficile però immaginare l'implementazione di una simile policy, dal momento che proprio l'uso di una rete privata virtuale dovrebbe impedire al governo di vedere cosa si sta facendo online. Dietro la norma, sembrerebbero esserci anche ragioni economiche: molti residenti degli Emirati usano le Vpn per accedere ad app messe al bando come WhatsApp e Viber, che permettono di comunicare attraverso Internet aggirando le costose tariffe telefoniche degli operatori tradizionali di telecomunicazioni. E che presentano l'aggravante – almeno alcune di queste – di non essere facilmente intercettabili.

"I leader politici qui sono ossessionati dalla sicurezza, e pensano che lo Stato abbia il diritto di arrivare anche a spiare le vite delle persone. Per loro è l'unica soluzione alle richieste di cambiamento sociale e politico", mi aveva detto Mansoor quando lo avevo sentito la prima volta, nel 2015.

Altri esempi di sorveglianza e censura

Anche il Bahrain ha fatto ampio uso di spyware comprati in Occidente per controllare e reprimere il dissenso, almeno fin dal 2012, come denunciato da varie organizzazioni, da Bahrain Watch al già citato Citizen Lab. Tuttavia nel luglio 2016, proprio mentre i vicini Emirati si apprestavano a completare la loro task force di sorveglianza a tappeto degli apparecchi connessi a Internet, il piccolo regno mediorientale testava una diversa forma di controllo delle comunicazioni.

Nel villaggio di Duraz, per alcune settimane, tutte le sere, spariva la

connessione Internet, sia quella via rete mobile sia quella via rete fissa. Il malfunzionamento è comparso tre giorni dopo l'inizio, nella zona, di una serie di proteste antigovernative. Gli operatori telefonici non hanno fornito spiegazioni al riguardo, ma un'investigazione dell'organizzazione Bahrain Watch ha suggerito che il problema fosse tutt'altro che casuale: un blocco temporaneo e iperlocalizzato delle connessioni come "una nuova forma di controllo dell'informazione".

Non è chiaro come ciò sia avvenuto, e dopo le prime denunce il blocco sembra essere diventato ancora più granulare, colpendo solo gruppi di residenti. Secondo Bahrain Watch, potrebbe essere stato usato un apparecchio che, dopo un'analisi del flusso di dati che passa da una dorsale, blocchi il traffico proveniente solo da (o diretto a) specifici indirizzi Ip.

Nel giugno 2016 l'Onu ha adottato una risoluzione che condanna l'interruzione o la limitazione dell'accesso a Internet da parte degli Stati. Ma chiudere la Rete su larga scala, a livello nazionale, per reprimere il dissenso – celebre fu il caso dell'Egitto nel 2011 – è un fatto plateale, lampante, visibile, che provoca per di più notevoli danni economici e vari problemi di mancata erogazione di servizi al pubblico. Farlo a livello locale e in modo mirato è invece più difficile da individuare e denunciare.

Ad agosto anche in Etiopia, in concomitanza con alcune proteste, si è registrato il blocco di Internet per almeno un weekend, come ha riferito la rivista "Quartz", anche se non è stata in grado di mapparne l'estensione, se cioè riguardasse tutto il Paese e tutte le reti o soltanto alcune regioni. L'organizzazione Access Now sta segnalando tutti i casi di interruzione di Internet o di alcuni suoi servizi registratisi nel mondo nel 2016: la lista è molto lunga.

Sempre nell'estate 2016, il Bahrain ha bloccato anche l'accesso a Telegram, l'app di messaggi cifrati. In questo campo però è stato surclassato, per sofisticazione, dall'Iran. Telegram è usato da 20 milioni di iraniani, uno su quattro, ed è diventato uno strumento per diffondere informazioni da parte delle forze di opposizione, anche grazie ad alcune sue funzionalità, come i gruppi e i canali. Inoltre offre la possibilità di avere conversazioni uno-a-uno cifrate end-to-end, come abbiamo già visto. Nel febbraio 2016 un articolo del "Guardian" sottolineava la crescente importanza della app di messaggistica nel Paese, aggiungendo come il governo avesse deciso, per il momento, di non bloccarla, diversamente da

quanto era successo con Viber, Twitter e Facebook.

In compenso, però, qualcosa di diverso si stava muovendo dietro le quinte. Degli hacker iraniani – un gruppo definito Rocket Kitten, probabilmente legato al governo –, sfruttando alcune falle della app, hanno identificato i numeri di telefono di 15 milioni di utenti iraniani – in pratica quasi tutti quelli che lo usavano. E hanno compromesso dozzine di account di attivisti. A denunciarlo è stata ad agosto una indagine di due ricercatori di sicurezza, Collin Anderson e Claudio Guarnieri. La vulnerabilità sfruttata dagli hacker per compromettere e violare decine di profili si basa sul sistema di attivazione degli account Telegram, che invia un sms con un codice di conferma ai nuovi iscritti. Ma questo codice può essere facilmente intercettato e utilizzato – specie in Paesi dove le società di telecomunicazioni sono sotto il controllo governativo – per aggiungere un nuovo apparecchio al profilo dell'utente preso di mira, così da poter leggere i suoi messaggi[29].

Naturalmente questi sono solo alcuni esempi recenti. Per molti Paesi – soprattutto dove non vige lo stato di diritto – sono emersi programmi o situazioni simili, e raccontarli tutti richiederebbe un libro a parte. Ma la diffusione di tecnologie per raccogliere o intercettare comunicazioni di ogni tipo, anche cifrate, è un dato di fatto che accomuna dittature e democrazie. Cambiano i contesti di utilizzo e le garanzie formali o sostanziali per controllare o limitare gli abusi delle stesse. Tutti dicono di usarle come strumento investigativo contro criminali e terroristi. Alcuni lo fanno, altri le sfruttano per spiare giornalisti o politici scomodi, per reprimere il dissenso, per stroncare mobilitazioni. Resta il problema, anche negli Stati di diritto, di come circoscrivere e monitorare l'utilizzo di certi strumenti; o di quali adottare e quali ritenere semplicemente inaccettabili. Nondimeno, la loro espansione è un fenomeno globale. E, mentre scrivo, i controlli quasi inesistenti ovunque.

I tanti modi per impossessarsi dei dati

Nella maggior parte dei casi, i dispositivi digitali sono dei colabrodi che si possono attaccare su più livelli. E per farlo non occorre essere l'Nsa e nemmeno la polizia giudiziaria. Perché le strade per ottenere dati utili dai nostri dispositivi sono tante, molte di più di quelle che normalmente

immaginiamo. Sono, inoltre, in continua evoluzione; e, a volte, alla portata di qualsiasi malintenzionato.

Per capirlo occorre fare un passo indietro, allo scontro Fbi-Apple. Quell'episodio e le contemporanee preoccupazioni sulla crittografia sollevate con la motivazione dell'emergenza terrorismo hanno prodotto, ovunque, un gran numero di incontri di informatica forense. Anche in Italia. Uno di questi, a cui ho partecipato nel maggio 2016 all'Università di Milano, raccoglieva la crema dei "Mr. Wolf" dei telefonini e dei pc. Di quelli, cioè, che vengono chiamati dalla polizia quando devono "risolvere un problema" di accesso a dati digitali: entrare in un computer o recuperare informazioni apparentemente inaccessibili. E gli informatici forensi arrivano e si mettono al lavoro, con scatolotti, valigette, cavi, laptop, come quelli che abbiamo visto in precedenza nello studio di Mattia Epifani. Che non a caso è uno dei relatori presenti anche al convegno milanese.

Partecipare a questo genere di incontri è molto istruttivo perché si capiscono due concetti fondamentali, che proverò a spiegare in modo più suggestivo che scientifico. Primo, i dati digitali sono tenacemente persistenti: anche quando pensiamo di cancellarli, nella maggior parte dei casi ciò non avviene. Secondo, anche se si ha un'auto da Formula 1 non si diventa automaticamente un grande pilota – fuor di metafora, anche strumenti potenzialmente molto sicuri devono essere usati e configurati in modo appropriato. Per farlo è necessario inanellare una serie di software, apparecchi, pratiche e conoscenze che non sono così banali. E dove l'errore umano resta il baco più diffuso.

Per riformulare quanto detto: se si frequentano gli allegri raduni degli informatici forensi, si capisce che la crittografia si è realmente estesa e rafforzata negli ultimi anni, grazie ad alcune aziende, software e app; e che ciò nonostante, smartphone e pc non sono diventati così inaccessibili come l'Fbi e altri ci vorrebbero far credere.

Ne danno una breve e semplice dimostrazione proprio i relatori del convegno milanese. A un certo punto dell'incontro, sullo schermo in sala appaiono i nomi di reti Wi-Fi sparse nel mondo: alcune sembrano essere di alberghi, altre probabilmente del posto di lavoro e di casa. Risatine nell'uditorio, perché quei dati apparsi in aula sono stati in realtà raccolti proprio dai pc e dagli smartphone dei presenti.

La pesca è stata fatta attraverso un apparecchietto dall'aria innocua, poggiato sul tavolo dei relatori. È un Wi-Fi Pineapple, si compra online per 99 dollari e si finge un "access point" noto per raccogliere i dati relativi alle reti Wi-Fi usate da smartphone e pc che stanno nelle vicinanze. Questi infatti lanciano ricerche di rete in continuazione e ingannarli attraverso un access point – un apparecchio che consente una connessione wireless – in realtà sconosciuto, ma in grado di accettare la loro richiesta di accesso come fosse quello di casa, è un gioco da ragazzi.

Tale genere di attacco si chiama "karma attack" e, nel suo livello più semplice, viene usato per rastrellare informazioni a scopo di intelligence, ad esempio per vedere chi partecipa a eventi pubblici anche lontani nel tempo, incrociando semplicemente i dati raccolti (ovvero le richieste con i nomi delle reti Wi-Fi usate dai dispositivi e i loro indirizzi Mac). Basta che i dispositivi abbiano il Wi-Fi attivo. Ma questo è solo il primo livello. "Se poi lascio anche 'autoconnect' attivo sul mio smartphone [l'opzione *Richiedi accesso reti*], quando il telefono cerca ad esempio la rete Wi-Fi Frecciarossa, usata durante un viaggio precedente, l'access point gli risponde facendo finta di essere quella rete. Allora il mio smartphone si connette all'access point falso e il traffico viene effettivamente inoltrato da e verso Internet, ma allo stesso tempo viene anche intercettato", mi spiega Paolo Dal Checco, che abbiamo già incontrato in precedenza e che è tra i relatori presenti in sala.

In pratica, se si inizia a navigare usando quell'access point, "ogni singolo pacchetto viaggerà attraverso tale dispositivo e conseguentemente potrà essere visualizzato, modificato, rediretto o 'droppato' [scartato] a discrezione dell'operatore", mi dice Margaritelli. Questo per quanto riguarda il traffico in chiaro, non cifrato. Ma a quel punto si può anche tentare un attacco sul traffico cifrato. Come si fa? In parte ne abbiamo già parlato all'inizio. Quando il target va sul sito Facebook.com o su Google.com, lo si reindirizza ad altre pagine simili, finte, da cui si copiano le credenziali di accesso ai siti originari se sono immesse dall'utente ignaro.

Me lo spiega ancora una volta Margaritelli: "Tutto ciò che l'attaccante può vedere fino a questo punto è il traffico non criptato, e può dedurre a quali siti https la vittima si sta connettendo. Per poter visualizzare il traffico criptato è necessario installare un certificato (del quale l'attaccante possiede anche la chiave privata) sul dispositivo e poi indirizzare tutte le connessioni

cifrate verso un server sotto il proprio controllo. La vittima penserà di connettersi a Facebook, ma in realtà sarà su un sito controllato dall'attaccante che, una volta visualizzati i dati (potendoli decriptare perché, ricordiamo, erano stati cifrati col suo certificato), la 'rimbalzerà' sul server originale". Il certificato si può installare attraverso un exploit, un malware o manualmente nel caso in cui l'attaccante abbia accesso fisico al dispositivo.

Quanto avvenuto in aula è solo una dimostrazione limitata e goliardica ad uso del pubblico, ma esistono sistemi molto più sofisticati per pescare dati. Ci sono apparecchi che fingono di essere un ripetitore di un operatore telefonico. Sono gli "Imsi catcher", usati per registrare, monitorare e localizzare tutti i tipi di telefonini presenti in una certa area, rubando i loro codici Imsi e Imei. Il codice Imsi identifica una sim all'interno della rete di un operatore telefonico. Il codice Imei identifica un dispositivo. Gli Imsi catcher si possono acquistare perfino da venditori cinesi sul sito Alibaba. Tra le caratteristiche descritte, anche la possibilità di impedire il funzionamento di un telefono.

Sono sistemi ampiamente usati da anni dalle polizie e dall'intelligence di tutto il mondo, specie in occasione di raduni e manifestazioni di vario tipo, dove la densità di dispositivi – e l'interesse per i loro proprietari – è molto alta. Per cercare utilizzi simili non serve andare lontano, basta guardare in casa. In Italia il bando di gara più recente del ministero dell'Interno risale a fine 2015: richiedeva la fornitura di due sistemi integrati per funzionalità Imsi catcher, ovvero per il "monitoraggio e localizzazione dei terminali radiomobili attraverso l'impiego di un unico kit trasportabile, impiegabile ed alimentabile con autoveicoli commerciali". Nel dicembre 2015 ad aggiudicarsi la gara è stata l'azienda Italarms per 649mila euro.

Tra gli Imsi catcher – negli Usa li chiamano "Stingray" – ce ne sono alcuni in grado di intercettare anche le comunicazioni voce e sms, localizzando fino a 10mila target in un'area. Ad esempio quelli prodotti da Drt, Digital Receiver Technologies (soprannominati "dirty boxes"), azienda del Maryland sussidiaria di Boeing, che li vende a 40mila dollari. Ogni Stingray varia di prezzo a seconda delle funzionalità e della portata di esercizio.

A fine 2015 l'associazione americana per i diritti civili Aclu, dopo una battaglia legale, ha ottenuto documenti governativi che mostrano come

alcuni di questi apparecchi – che negli Usa sono stati spesso usati in segreto e senza mandato di un giudice – siano effettivamente in grado di intercettare anche telefonate e sms. Oltre che di bloccare temporaneamente le comunicazioni mobili.

Questo genere di strumenti sono dunque ampiamente usati negli Stati Uniti e in Canada, ma le circostanze del loro effettivo utilizzo sono oscurate da una cortina di segretezza. Diversi attivisti e giornalisti hanno fatto ricorso ai tribunali, dopo una prima richiesta attraverso la legge (il Freedom of Information Act, o Foia) che garantisce il diritto di accesso a informazioni statali. Così nel gennaio 2016 un giudice statunitense ha ordinato alla polizia di Chicago di mostrare i documenti che spiegavano pienamente il loro impiego degli Stingray (o Imsi catcher), in virtù di una richiesta avanzata da un attivista nel 2014. Dove, come, quando, perché, con quali direttive e procedure sono usati questi strumenti? E rispettano le leggi costituzionali? Erano queste le domande cui si voleva dare una risposta.

Un mese dopo è emerso – grazie a documenti ottenuti, sempre attraverso le leggi americane, da un'altra organizzazione per i diritti civili, la Nyclu – che la polizia di New York aveva usato degli Stingray per più di mille volte dal 2008. Eppure soltanto nel febbraio 2016 le forze dell'ordine hanno per la prima volta ammesso pubblicamente di usarli, obbligate dal Freedom of Information Act e da un giudice. Tra le altre cose, è affiorato il fatto che la polizia newyorchese non doveva ottenere il mandato di un magistrato per rastrellare dati con questi apparecchi. Bastava ottenere la stessa autorizzazione prevista per accedere ai tabulati di un telefono ("pen register order"), senza che dovessero esserci fondati indizi di colpevolezza. Inoltre, la polizia non sembrava avere un documento scritto che descrivesse le condizioni d'utilizzo di tali strumenti.

Gli Stingray nascono nel 2003, inizialmente per impieghi militari. Ma come spesso accade con le tecnologie di intercettazione e sorveglianza, da lì sono tracimati nell'ambito civile e sono stati adottati in ordine sparso dalle forze dell'ordine. Secondo dati di metà 2016 della Aclu, tali apparecchi erano impiegati da almeno 59 dipartimenti di polizia, in 23 Stati degli Usa, oltre che da 13 agenzie federali – incluse la Dea (l'antidroga), l'Fbi e l'Irs, ovvero l'agenzia delle entrate. Ma si tratta di una stima per difetto.

"I simulatori di ripetitori cellulari sono potenti strumenti di sorveglianza che possono tracciare le persone, anche dentro le loro case, e raccogliere informazioni da cittadini innocenti che si trovino nei paraggi", ha dichiarato nel 2016 Mariko Hirose, un legale della Nyclu. "Se sono impiegati all'interno di comunità, la polizia dovrebbe come minimo ottenere un mandato e seguire delle direttive scritte nero su bianco". Al contrario, l'Fbi si premurava di far firmare ai dipartimenti locali di polizia degli accordi di segretezza sull'uso degli Stingray, con la motivazione che criminali e terroristi avrebbero potuto adottare delle contromisure se avessero saputo della loro esistenza.

Nell'estate 2016 anche la polizia di Vancouver, in Canada, sempre in seguito all'azione legale di gruppi per i diritti civili, è stata costretta ad ammettere l'uso di Stingray. I primi utilizzi risalivano a circa dieci anni prima e non prevedevano un mandato. E in precedenza era emerso che anche la Royal Canadian Mounted Police, cioè l'Fbi canadese, aveva usato Imsi catcher per oltre una decade, raccogliendo informazioni su migliaia di canadesi.

Negli ultimi tempi si sono diffusi anche degli apparecchi di nuova generazione che, sfruttando proprio la funzione di ricerca e accesso alle reti Wi-Fi dei dispositivi, promettono di fare qualcosa di più degli Imsi catcher. Prodotti soprattutto da aziende israeliane come Rayzone, Wintego e Magen, sostengono di essere in grado di sottrarre a dispositivi presenti in una certa area – e con Wi-Fi attivo – password, lista contatti, Dropbox, foto e cronologia della navigazione col browser. La loro viene chiamata intercettazione via cloud e avverrebbe sfruttando alcune vulnerabilità delle app, almeno secondo le brochure dei produttori.

In questo scenario, si dà per scontato che le tradizionali chiamate vocali siano facilmente intercettabili. Di solito però ciò avviene – o dovrebbe avvenire – attraverso la polizia giudiziaria, in collaborazione con un operatore telefonico e con il mandato di un giudice. Eppure esistono tecnologie che permettono di saltare questo passaggio. Un'azienda israeliana di nome Ability offre infatti un servizio in grado di intercettare qualsiasi telefonata e sms di qualsiasi telefono in qualsiasi posizione geografica si trovi – dunque senza la necessità, come con i vari Imsi catcher, di essere nelle vicinanze; e senza quella di ottenere la collaborazione di una compagnia di telecomunicazioni come nelle

intercettazioni vecchio stile.

Questo sistema – chiamato Ulin (Unlimited Interception System) – non dipende dall'operatore telefonico, né da limiti geografici o confini nazionali: richiede solo di sapere il codice Imsi di un telefono. Funziona sfruttando una vulnerabilità di SS7 (Signalling System 7), un vecchio insieme di protocolli usati per connettere gli operatori telefonici globali e sulle cui vulnerabilità negli ultimi tempi si è sviluppata una sorta di industria a sé stante. Il sistema però appare piuttosto costoso – fino a 20 milioni di dollari a seconda del numero di target – e rivolto soprattutto all'intelligence. Inoltre, non riuscirebbe ad intercettare chiamate dati realizzate attraverso app che proteggono la comunicazione con crittografia end-to-end.

A superare le difese della crittografia ci pensano invece i trojan, che sono diventati uno degli strumenti investigativi più diffusi – ma fino a qualche tempo fa poco noti – degli ultimi anni. Una volta installato su uno smartphone, tablet o pc, il trojan può essere usato per spiarne tutta la sua attività (comunicazioni telefoniche, mail, chat, foto, Skype, navigazione web, file e documenti), nonché per attivare microfono e videocamera in modo da effettuare intercettazioni ambientali.

Esso viene definito trojan per indicare questa sua capacità di infettare un dispositivo; spyware per specificare quello che fa una volta installato, ovvero spiare. Si tratta dello stesso tipo di software usato anche dai cyber-criminali – anche se varia il livello di sofisticazione. Quando viene usato dallo Stato per effettuare indagini, viene ribattezzato captatore informatico, agente intrusore o virus autoinstallante. È uno strumento molto potente, dalle molte implicazioni, anche tecniche, e su cui vige un tabù, nel senso che lo si usa ma nessuno (o quasi) ne parla volentieri.

Il primo utilizzo documentato in Italia risale al 2004. Bisogna aspettare però il 2010 perché esso venga alla luce, attraverso una sentenza. Nel 2011 il tema appare sulla stampa italiana grazie all'inchiesta sulla cosiddetta P4, e nello stesso anno il noto gruppo di hacker tedeschi Chaos Computer Club scopre l'uso di un trojan da parte della polizia federale in Germania. Nel 2012-13 il tema riemerge in Stati come il Bahrain, gli Emirati e l'Etiopia, dove alcuni di questi spyware sono stati rinvenuti sui pc di attivisti, giornalisti e avvocati. Ma sembrerebbe restare un problema di utilizzo improprio da parte di Stati autoritari che comprano i trojan/spyware da

aziende occidentali. Del loro utilizzo negli Stati di diritto non si fa cenno, se non in alcuni convegni di specialisti e integralisti della privacy.

Sarà solo l'attacco informatico subìto nell'estate 2015 dal produttore italiano di spyware Hacking Team a portare il tema al grande pubblico, mostrando come i trojan fossero adottati da anni da servizi di intelligence e forze dell'ordine nazionali per le attività di indagine, dalla criminalità organizzata al terrorismo. Ma anche per sospetto peculato o corruzione.

Non sembra esserci infatti un limite per tipologia (o gravità) di reato. E ancora non sembra esserci un modo (o comunque, se c'è, non è stato adottato) per segmentare le funzioni di questi virus, cioè per fare in modo che siano usati per intercettare una singola telefonata su Skype o WhatsApp. O per impedire che sia attivata la videocamera. O che una registrazione audio o video avvenga in camera da letto. O che il virus effettui una perquisizione su anni di documenti e mail di qualcuno, quando il mandato iniziale era di intercettare soltanto le comunicazioni di un ristretto periodo di tempo. O per garantire che quanto acquisito non sia stato alterato o manipolato nelle varie fasi. L'impiego dei trojan e le domande che sollevano sono rimasti a galleggiare per anni nel silenzio ovattato delle istituzioni, delle aziende che erano interessate a vendere e non dovevano porsi troppe domande, e di un limbo giuridico che assomigliava a un Far West *de facto*.

Mentre scrivo, in Italia sono state avanzate alcune proposte di legge per provare a regolamentare il loro utilizzo. C'è chi teme che una legge conduca al loro sdoganamento definitivo. E chi la intende come l'unico modo per arginare strumenti fuori controllo. Ma le leggi sapranno definire tecnicamente cosa possa fare o meno un software di questo tipo? Riusciranno a mettergli dei paletti? E come?

La questione è al centro di un intenso dibattito fra gli addetti ai lavori e mostra, una volta per tutte, la rilevanza di conoscere e capire il funzionamento di tecnologie complesse e delicate anche al fine di prendere decisioni politiche. O saranno le tecnologie stesse a spingere la politica – e il diritto – nella direzione che vorranno.

Del resto, la frontiera della sorveglianza non è mai stata così dinamica, anche in termini di business e aziende. "Oggi numerose società hanno iniziato a offrire pacchetti completi: non solo prodotti ma anche molto training, sia nell'ambito informatico che nell'ambito fisico", mi racconta

una persona del settore di ritorno dalla fiera europea dell'Iss, tenutasi a Praga nel giugno 2016.

"Ci sono anche società, come l'indiana ClearTrail, che propongono una sorta di 'market place', di negozio online, dove le polizie possono acquistare prodotti di security su Internet, come se fosse un AppStore. La vera novità della fiera, tuttavia, è stata la massiccia presenza di società israeliane fra gli espositori; alcune di queste dichiaravano apertamente di venire da Israele, altre cercavano di mascherare la loro provenienza utilizzando dei rappresentanti europei; in generale sembra che le loro tecnologie siano complementari e, in alcuni casi, sembra anche che sfruttino delle sinergie tecnologiche e logistiche". Mi fa i nomi di alcune delle aziende che spiccavano. Alcuni li abbiamo già incontrati: come Ability, che fornisce un prodotto in grado di utilizzare le debolezze del protocollo SS7 per poter intercettare le telefonate e gli sms, e individuare la posizione di qualsiasi telefono nel mondo (anche se "con prezzi esorbitanti", commenta la mia fonte).

La loro tecnologia farebbe da supporto anche ai sistemi di un'altra azienda israeliana, Nso, che, come abbiamo già visto, è produttrice di spyware. Nso asseriva di poter infettare iOS aggiornati all'ultima versione senza interazione da parte dell'utente. "Continua ad avere dei prezzi molto superiori alla media, ma sta cercando di imporsi come leader indiscusso nel campo dei trojan su piattaforme iOS e Android", mi dice ancora l'esperto di sicurezza, che preferisce restare anonimo.

Poi c'erano aziende come Rayzone o Equus, con i loro prodotti in grado di estrarre dati dai dispositivi mobili sfruttando delle configurazioni "deboli" dei client, senza la necessità di installare un trojan. Ma nel programma dell'Iss di Praga c'era anche tanta cyber-intelligence. Come quella realizzata da Fifth Dimension: "Il loro prodotto sembra essere studiato per identificare minacce digitali sconosciute ed effettuare un'analisi predittiva su dati provenienti dalle fonti più disparate", racconta ancora la mia fonte. "Tuttavia non hanno mostrato nulla del loro prodotto se non in sessioni private a clienti selezionati".

La visibilità di massa e la trasparenza non sono esattamente la prima esigenza degli attori di questo mercato.

[27] Semplificando, un client è un terminale o un programma che si interfaccia con un altro – il server – che fornisce dei dati o un servizio (un sito, una casella di posta, ecc.).

[28] I protocolli http e https permettono lo scambio di informazioni fra due nodi della Rete, ovvero le richieste dei client e le risposte del server. Con http le comunicazioni sono in chiaro, cioè sono leggibili da chi intercetti il traffico. Https – che sta per "Http Secure", cioè "sicuro" – stabilisce invece un canale di comunicazione protetto dalla crittografia.

[29] Nelle impostazioni della app si può però verificare quali sono gli apparecchi collegati; inoltre si può inserire una ulteriore password di sicurezza per arginare questo specifico rischio.

8.
Tor, o della complessità delle cipolle

Tutte le sfide di Tor

Per chi sviluppa software per l'anonimato, anche raccogliere dati sui propri utenti costituisce un problema. È quanto mi spiega Roger Dingledine, quando cerchiamo di fare il punto su quante persone al mondo usino Tor. Si tratta del noto software che permette di navigare il web o di comunicare con qualcuno difendendo la propria identità e privacy; ma anche di realizzare siti anonimi e non localizzabili, che vanno a formare l'ossatura principale delle darknet, le reti "oscure" in quanto non indicizzate dai motori di ricerca e raggiungibili solo attraverso speciali software, che sui media diventano il cosiddetto Dark Web.

Dingledine è uno degli architetti originari del progetto Tor, e quando lo incontro, nella primavera 2016, continua ad esserne, ad oltre dieci anni dalla nascita, lo sviluppatore capo e il presidente. Non è ancora scoppiato il "Torgate", un presunto scandalo a sfondo sessuale, con reciproche e violente accuse di aver montato macchine del fango da parte di alcuni membri del progetto, e con divisioni e attriti propagatisi alla comunità di attivisti che porteranno addirittura alcuni (una minoranza, in verità) a proclamare uno sciopero di Tor – nonché a chiedere le dimissioni dello stesso Dingledine.

Nel momento in cui parliamo, Tor – più che con le sue tensioni interne – deve vedersela con i nemici esterni. Alcuni sono molto potenti. Anche se, come vedremo, il progetto ha anche amici altrettanto formidabili. Ed è proprio per questo, cioè proprio per il fatto di non essere facilmente incasellabile nelle semplificazioni giornalistiche e politiche con cui siamo

abituati a trattare i fenomeni tecnologici, che questo software, e chi ci lavora, sono così interessanti. E paradigmatici.

Dicevamo di Dingledine. Laureatosi in informatica al prestigioso Massachusetts Institute of Technology (il Mit di Boston), divenuto un ricercatore specializzato in software per pubblicare contenuti in modo anonimo e distribuito[30], è tra le tre persone che hanno sviluppato Tor, traghettandolo dalle sue prime origini nell'alveo di un progetto di ricerca militare (come vedremo tra poco) fino alla società civile, cioè a una comunità di attivisti, associazioni, sviluppatori e ricercatori.

Dingledine – che oggi ha circa 45 anni, una lunga coda di cavallo, un'aria da ragazzo studioso e un understatement quasi britannico – ha dunque dato vita a uno dei più efficaci strumenti a disposizione di dissidenti, minoranze e giornalisti per proteggersi online. Ma, soprattutto negli ultimi anni, ha dovuto fare i conti anche con l'accusa, da parte di alcuni rappresentanti di governi e forze dell'ordine, che software come questo agevolino criminali e malintenzionati. Accuse che abbiamo già incontrato nei capitoli precedenti ai danni dei maggiori strumenti di cifratura o anonimato.

"Sono oltre 2 milioni gli utenti che ogni giorno usano Tor, ma è una cifra per difetto, perché non abbiamo trovato un modo per raccogliere dati più accurati sugli utilizzatori senza metterli in qualche modo a rischio", mi dice mentre siamo seduti nella biblioteca dell'Internet Freedom Festival di Valencia. Poco più in là, sparsi fra i tavoli, mescolati agli altri attivisti, ci sono numerosi membri di Tor: sviluppatori, operatori di suoi nodi o di progetti correlati.

"Molti di questi utenti arrivano da Paesi come la Turchia, l'Uganda, la Russia. Diciamo che periodicamente ti accorgi di quando censurano siti come Facebook perché hai una impennata nell'utilizzo di Tor. In passato abbiamo assistito a simili punte in Egitto, Tunisia, Siria, Iran". Già, perché Tor, oltre a renderti anonimo, ti permette di aggirare filtri, blocchi e censure online. "Di tutto questo traffico solo il 5 per cento è diretto ai siti o servizi nascosti [il cosiddetto Dark Web]. Ogni tanto esce uno studio che dice che questo genere di siti contiene solo contenuti illegali e odiosi, ma la realtà è che solo una sconosciuta frazione di questo 5 per cento è traffico diretto verso contenuti di tipo criminale. Senza contare che questi studi non sono in grado di conteggiare molti usi legittimi di Tor, ad esempio

quando ci sono persone che lo impiegano per comunicare fra loro attraverso software come Ricochet [un sistema di messaggistica cifrato e decentralizzato]. O per trasmettere file in modo sicuro", prosegue Dingledine.

Ci passa vicino Shari Steele, la nuova direttrice esecutiva di Tor, arrivata dopo anni di attivismo alla Electronic Frontier Foundation con due obiettivi principali: raccogliere e diversificare i fondi; ribadire che questo software fa parte dell'album di famiglia dei difensori dei diritti umani.

Tor è entrato nel mirino di chi vede in anonimato e crittografia un rifugio per terroristi, dico a Dingledine. "Il punto è che Tor non è utile per i terroristi", risponde lui. "Mi spiego: è uno strumento aperto, analizzato dalla comunità, e sviluppato per un utilizzo da parte di milioni di persone, utenti normali che altrimenti non avrebbero altri mezzi per proteggersi. Invece, per chi abbia cattive intenzioni ci sarebbero comunque molte altre alternative a disposizione: strumenti molto più invisibili, anche temporanei, per gruppi ristretti, che non hanno un problema di scala come il nostro, che cioè non devono essere utilizzabili da milioni di persone e durare nel tempo". Mentre gli sviluppatori di Tor combattono tutti i giorni: contro i censori della Cina e dell'Iran, ad esempio. "Abbiamo adottato un sistema per non far riconoscere il traffico di Tor, lo mimetizziamo come qualcosa d'altro, altrimenti chi fa analisi dei pacchetti potrebbe bloccarlo".

Storia di un progetto complesso

Ma Dingledine e i suoi devono fronteggiare anche le iniziative del Dipartimento della Difesa Usa o dell'Fbi, che ad esempio hanno finanziato una università americana per sviluppare un tipo di attacco contro gli utenti di Tor. E pensare che "l'80 per cento dei nostri finanziamenti arriva ancora dal governo americano", mi dice Dingledine.

Non è un segreto. Anzi, è uno di quei temi che vengono di tanto in tanto riproposti dai detrattori di questo software, per affermare che non è sicuro. Come si fa a fidarsi – dicono i suoi critici – di un progetto in larga parte finanziato dal governo americano? Lo stesso del Datagate, della Nsa, di un'intelligence basata sul principio del "raccogli tutto" (riferito alle comunicazioni digitali), del braccio di ferro con Apple sulla crittografia,

della prima cripto-guerra, dell'uso di vulnerabilità sconosciute per entrare in router e dispositivi prodotti anche da aziende statunitensi? E la lista di esempi potrebbe continuare. Ma prima di tirare la volata a facili complottismi, occorre prendere in considerazione la nascita di Tor e la complessità del panorama socio-tecno-politico in cui è immerso.

È il 1995, quello che è considerato il primo anno della diffusione commerciale del web. L'anno prima Netscape ha rilasciato il suo browser Navigator; e ora Microsoft ha lanciato Internet Explorer 1 e Windows 95; Google non esiste ancora. È un anno importante per la Rete, ma lo è anche per quella che verrà chiamata l'Internet nascosta. L'ufficio di Ricerca navale americano (Onr) finanzia infatti i Laboratori di ricerca navale (Nrl) della Marina per sviluppare l'"onion routing". L'espressione indica una tecnica per comunicare in modo anonimo attraverso una rete dove i messaggi sono incapsulati in più strati di cifratura che sono tirati via come quelli di una cipolla ("onion", in inglese) a mano a mano che rimbalzano fra i diversi nodi ("router") della rete fino ad arrivare alla fine. Ogni nodo toglie solo uno strato di cifratura in modo da conoscere l'immediata destinazione successiva, cioè il nodo seguente cui mandarlo, ma non quella finale, che sarà nota soltanto all'ultimo nodo. Chi invia il messaggio resta anonimo perché ad ogni passaggio il nodo che smista il traffico nel corso dei vari rimbalzi per questa rete saprà solo l'indirizzo immediatamente precedente e quello immediatamente successivo.

Tale tecnica – chiamata appunto onion routing – è stata sviluppata a metà degli anni Novanta da tre ricercatori dei Laboratori di ricerca navale della Marina americana – Paul F. Syverson, Michael G. Reed e David M. Goldschlag – nell'ambito di sperimentazioni volte a proteggere l'identità e le comunicazioni di chi lavorava nell'intelligence. Ci sono delle slide di Syverson che mostrano come potesse essere utilizzata se un agente americano si fosse trovato in un Paese ostile e repressivo (Repressia, lo chiama). Come poteva navigare dalla sua stanza di hotel sui siti del Pentagono o comunicare con i suoi superiori senza essere individuato? O come faceva anche solo a raggiungere tali siti, se questi erano filtrati e censurati in quel Paese? Altri casi d'utilizzo erano la raccolta di informazioni di intelligence da fonti aperte senza farsi individuare; l'incoraggiamento di soffiate anonime; e l'investigazione di criminali. Ma anche l'apertura di un canale di comunicazione diretto coi cittadini. E,

ancora, la protezione di normali utenti da molestie online o dallo stalking, anche digitale, di ex partner; o la sorveglianza di aziende private.

Esattamente come Internet, Tor è stato concepito in seno alla Difesa statunitense con un finanziamento della Darpa, l'agenzia militare che progetta e inventa nuove tecnologie. All'inizio degli anni Duemila, arrivano anche Dingledine e un altro ricercatore, Nick Mathewson, che insieme a Syverson si mettono a sviluppare una seconda implementazione dell'onion routing, quella che verrà chiamata appunto Tor (acronimo di "The onion routing"). Nel 2003 i Laboratori di ricerca navale rilasceranno il codice del progetto sotto una licenza libera (vuol dire che il codice è aperto, visionabile, scaricabile, modificabile, ridistribuibile gratuitamente da chiunque) e nel 2004 arriva il primo sostegno economico dall'associazione per i diritti digitali Electronic Frontier Foundation. A quel punto Tor – che all'epoca ha solo 100 nodi o "relay"[31] sparsi su tre continenti – si emancipa dalle sue origini statali, e mentre l'Ufficio di ricerche navali interrompe i finanziamenti, il progetto diventa una no-profit nel 2006. A distanza di pochi mesi la Nsa prende nota, e pubblica il suo primo studio interno su Tor.

Negli anni il progetto riceverà sostegno e denaro dall'Omidyar Network (fondo di investimenti filantropici del creatore di eBay Pierre Omidyar), da Google, dall'agenzia di cooperazione allo sviluppo svedese (Sida), dalla Knight Foundation (fondazione che sostiene progetti giornalistici di eccellenza e al servizio delle comunità come ProPublica), oltre che da molti privati e piccoli donatori. Ma i soldi provenienti da diverse agenzie statali statunitensi – in particolare dal Dipartimento di Stato, dalla National Science Foundation, dall'Agenzia per lo sviluppo internazionale, dall'International Broadcasting Bureau e addirittura da un ramo del Dipartimento della Difesa – ammonteranno sempre tra il 68 e il 93 per cento del budget totale.

Questo aspetto, unito al profilo storico di alcune delle citate agenzie – in particolare dell'International Broadcasting Bureau, parte del Broadcasting Board of Governors (Bbg), un ente federale la cui missione è "informare e connettere le persone nel mondo per promuovere libertà e democrazia", finanziatore di molte radio estere come Voice of America e Radio Free Asia considerate da alcuni semplicemente come il megafono della propaganda a stelle e strisce nel mondo –, è il tallone d'Achille principale di

Tor di fronte ai suoi critici.

Tuttavia i complottismi si sono sempre scontrati contro due fatti. Il primo è il codice su cui si basa Tor, aperto e controllato da centinaia di sviluppatori indipendenti in tutto il mondo, per cui possibili tentativi di inserirvi backdoor in modo da comprometterne di nascosto le funzioni dall'interno verrebbero prima o poi alla luce. Il secondo sono gli stessi documenti interni della Nsa, rilasciati da Edward Snowden ai media, secondo i quali Tor "puzza", nel senso che costituisce un ostacolo allo sforzo di raccogliere informazioni e identificare utenti da parte dell'agenzia americana. Che pur sviluppando alcuni attacchi mirati, riconosce di non essere in grado di deanonimizzare tutti i suoi utenti.

Così stando le cose, se per la Nsa Tor è un problema al punto da finanziare ricerche per bucarlo, perché allora il governo americano lo sostiene? Non solo per la ragione che l'espressione "governo americano" indica tutto fuorché un monolite, rappresentando al suo interno anime, esigenze e obiettivi spesso diversi. Ma anche perché strumenti come Tor e simili si sposano con una corrente importante della politica estera statunitense, quella basata sul concetto di "soft power" (di cui, a livello tecnologico, spiccano figure come quella di Alec Ross, ex consigliere di Hillary Clinton), in cui la proiezione del potere e dell'influenza di Washington si legano alla promozione della circolazione di informazioni, e al conseguente sostegno a movimenti di opposizione, in vari Paesi e regioni estere.

Per capirci: nel 2012 Radio Free Asia, a sua volta parte della già citata agenzia federale Bbg, dà vita a un nuovo fondo per sostenere progetti tech, l'Open Technology Fund. La sua missione è finanziare software e sistemi che promuovano la libertà di espressione e comunicazione, la lotta a forme di censura, la difesa dalla sorveglianza nel mondo. Questo fondo contribuisce non solo a Tor, ma anche ad altri software adottati da tempo da attivisti, testate tradizionali e singoli giornalisti, cripto-entusiasti, dissidenti di vari Stati, anticapitalisti, libertari, esperti di sicurezza informatica d'ogni credo, comuni utenti occidentali che vogliono visitare siti imbarazzanti e via dicendo. Software quali Signal, CryptoCat (altro software per comunicare in modo cifrato), Globaleaks (la piattaforma basata sul Dark Web per realizzare siti di "whistleblowing"[32] anonimi, alla Wikileaks), Tails (il sistema operativo per essere il più possibile anonimi e

sicuri), Qubes OS (il sistema operativo che promette di difenderti più di altri dal rischio di attacchi informatici), Orbot e Orfox, app per Android per comunicare o navigare proteggendo la propria identità, per citare i più noti.

Dunque, non solo Tor è in buona compagnia ma, considerata la sua importanza, rappresenta anche il cuore di molte contraddizioni legate a questo mondo: collegato inizialmente ai progetti di ricerca militare statunitensi, poi passato a una comunità internazionale composta fra gli altri da attivisti pro-privacy e anarchici; finanziato da un braccio del governo americano, attaccato da un altro; realizzato da sviluppatori che periodicamente da una parte vengono accusati di creare strumenti usati dai terroristi, e dall'altra vengono invitati da intelligence e forze dell'ordine a tenere seminari per imparare a usare quegli strumenti a fini investigativi; utilizzato dagli attivisti siriani anti-Assad o da quelli che documentano gli orrori dell'Isis per salvarsi la vita, così come da cyber-criminali d'ogni risma. Tor rispecchia perfettamente la complessità degli scenari tecnopolitici che ci troveremo sempre più spesso a dover districare. E non è detto che alla fine si trovino sempre risposte chiare e univoche.

Mentre scrivo, questo progetto è considerato lo standard dei sistemi di comunicazione anonimi, per efficacia e diffusione (ne esistono anche altri, come I2P, GNUnet, Freenet e anoNet). La sua rete distribuita e autogestita di nodi – sono 10mila, localizzati in 84 Paesi, gestiti da volontari sui propri pc – è usata da 2,5 milioni di utenti al giorno. I servizi nascosti – ovvero siti web, servizi di chat, ecc. che si basano sulla sua infrastruttura, e quindi formano il Dark Web – sono stimati sui 60mila. Quindi, una realtà relativamente contenuta, specie se comparata al resto del web.

Mutamenti e controversie

Tor sembra dunque incontrare ancora i favori di una parte dell'amministrazione americana. Tuttavia, le preoccupazioni per i continui tentativi di attacco da parte di Fbi e Nsa, così come per uno scenario politico che potrebbe mutare sotto la spinta di demagogie e attacchi terroristici, hanno messo la sua comunità sotto una pressione crescente.

Di qui una serie di mutamenti, a cominciare da un cambio ai vertici nella

gestione del progetto, con l’arrivo di una nuova direttrice esecutiva, Shari Steele, nel dicembre 2015. Steele non è una estranea: è stata per 15 anni alla guida della Electronic Frontier Foundation, la nota associazione americana per i diritti digitali che abbiamo già visto essere strettamente legata al progetto Tor fin dalle sue origini. “Tor è parte di una più ampia famiglia di organizzazioni per le libertà civili, e questo passaggio chiarisce la sua centralità all’interno di questa famiglia”, scriverà Dingledine sul blog del progetto. Quindi una scelta nel segno della continuità, ma probabilmente con una maggiore attenzione a diversificare la platea cui si rivolge e la stessa raccolta fondi.

“La diversità è una delle parole ricorrenti in questa comunità”, mi racconta Cristian Consonni, un operatore italiano di due nodi Tor. “La diversità si riferisce a chi gestisce i nodi, ai Paesi in cui si trovano, ai ‘provider’ cui si appoggiano”. Una diversità che ha ragioni tecniche e di sicurezza (diversamente la rete Tor sarebbe più facilmente attaccabile), ma che si traduce in una varietà anche sociale. Del resto, si dice, “l’anonimato ama la compagnia”: più persone e utenti, diversi fra loro, usano questo software, anche se non sono in pericolo di vita, più chi la rischia davvero viene protetto dal network.

Chiunque può scaricare il software e, oltre a usarlo, farlo diventare un nodo (relay) della rete Tor. Come Cristian, che due anni fa ha prima messo in piedi un nodo intermedio (“middle relay”) e poi un nodo di uscita (“exit node”). Ha affittato un server privato virtuale su Aruba e ci ha piazzato un exit node, il più delicato dei tre tipi di nodi di Tor (di entrata, middle o intermedi, e di uscita). In Italia ce ne sono solo sette di questo genere. “Mentre gestire un nodo intermedio non dà alcun problema, perché tutto quello che ci passa è cifrato, quello di uscita è più rognoso”, mi dice. Perché è il punto in cui il traffico esce dal tunnel cifrato della rete Tor per andare alla sua destinazione finale. E quindi un attore malevolo – l’intelligence o lo stesso operatore del nodo – potrebbe spiare il traffico in uscita, non più cifrato. Pur non sapendo da dove arriva, è in grado di vederne i contenuti (a meno che questi non siano a loro volta cifrati). “Ovviamente non lo faccio, perché è contrario ai miei principi, e perché il mio atteggiamento verso il traffico che passa dal mio nodo è agnostico; offro un servizio, esattamente come un provider”.

Non tutti però capiscono il ruolo degli operatori dei nodi Tor, e questo

potrebbe portare a grane legali nel caso in cui dal suo server passi del traffico riconducibile ad attività criminali. Qualcuno potrebbe andare a bussare alla sua porta e chiedergliene conto. È già successo, in Italia. Cristian ne è consapevole, ma dice che finora ha avuto soltanto quattro segnalazioni inviategli da Aruba per problemi minori, "spam-bot" che passavano dal suo server e cose simili.

Ad ogni modo, la sua è una scelta etico-politica. Pensa che gestire un nodo Tor e contribuire alla sua rete aiuti la difesa della privacy e a tenere in piedi uno strumento utilizzato da tante persone, in Paesi non democratici o in contesti difficili, per proteggersi. Lui è un dottorando in informatica all'Università di Trento ed è anche vicedirettore di Wikimedia Italia, sebbene l'attività di operatore Tor la svolga a titolo personale. "La decisione l'ho presa leggendo un articolo su Snowden, in cui lui raccontava di quando si era reso conto che le segnalazioni interne che aveva fatto alla Nsa sulle storture cui aveva assistito non avrebbero portato a niente, e che dunque doveva essere lui ad agire. E allora mi sono chiesto: cosa posso fare io per difendere la privacy?".

Cristian aveva già una visione di Internet come di uno strumento per esprimere il proprio pensiero. "Idealistica, se vuoi", mi dice, "poiché sappiamo come tale visione sia messa a rischio dalla concentrazione degli utenti su pochi servizi online, dalla sorveglianza corporate e governativa. Ma la mia idea è sempre stata di usare l'informatica per far avanzare i diritti umani: l'istruzione attraverso Wikimedia; la privacy attraverso Tor". Certo, in quanto strumento che consente un certo livello di anonimato, può essere adottato da chiunque, per scopi positivi o negativi. "A volte me lo chiedo, da operatore di un nodo: sto aiutando più i buoni o i cattivi? Per ora sono convinto che i vantaggi per i buoni siano superiori al fatto che ci possano essere anche dei cattivi che lo usano. Ma è una domanda che mi pongo, ovviamente".

E non è il solo a porsi questa domanda.

Nel maggio 2016, una delle sviluppatrici di Tor, nota come Isis Agora Lovecruft, anarchica, è letteralmente scappata dagli Stati Uniti, andando a rimpolpare una crescente comunità di attivisti a Berlino, dopo essere stata contattata più volte da agenti dell'Fbi. La ragione ufficiale di queste visite era ottenere la sua collaborazione in un caso di hacking a cui, secondo gli investigatori, la donna sarebbe stata connessa. In pratica, gli agenti

avrebbero voluto farla testimoniare in una indagine di cui però non si conoscevano i dettagli.

Nel 2016 sono anche emerse delle nuove procedure e tecniche investigative dell'Fbi che consistono, in buona sostanza, nell'hackerare i computer di migliaia di utenti Tor, presumibilmente connessi a un indagato o visitatori di un determinato sito, con un solo mandato di un giudice a disposizione. Sappiamo che ciò si è verificato almeno in un caso, sfruttando vulnerabilità note di Tor Browser, ma evidentemente non ancora "rattoppate" da alcuni utenti – al tempo dell'indagine non erano stati ancora introdotti gli aggiornamenti automatici di questo software. Il caso in questione ha riguardato utenti di un sito pedopornografico, e difficilmente ciò riesce a destare scandalo. Ma nulla vieta che lo stesso sistema, basato su un hackeraggio di massa, possa essere applicato anche in casi diversi e per sospetti di reati meno ripugnanti.

Il Jakegate e la crisi interna di Tor

In questo quadro, può risultare sorprendente che nel 2016, a gettare Tor in fibrillazione, molto più dei federali e degli attacchi informatici ai suoi utenti, sia stata una vicenda interna.

A fine maggio Jacob Appelbaum, hacker e attivista dei diritti digitali, già membro di Wikileaks, ma soprattutto, per quattro anni, il volto pubblico di Tor, sempre presente sui palchi delle conferenze di sicurezza informatica o di privacy, viene estromesso dal progetto nel mezzo di un polverone. A darne l'annuncio è lo stesso blog di Tor in due diversi post, dove si legge che "una serie di persone hanno pubblicamente avanzato delle gravi accuse di molestie sessuali da parte del nostro ex dipendente Jacob Appelbaum". Da quel momento si scatenano una serie di eventi che rendono la vicenda particolarmente scivolosa e intricata. Appelbaum viene infatti accusato, oltre che dal comunicato di Tor, da un sito anonimo che raccoglie testimonianze di presunti abusi da lui commessi su varie persone. Nonché da un profilo Twitter anonimo che lo invita addirittura al suicidio. Diverse organizzazioni a cui lui era legato, dalla Freedom of the Press Foundation a due autorevoli gruppi di hacker, Chaos Computer Club e Cult of the Dead Cow, lo espellono.

Appelbaum, dopo un primo momento di silenzio, reagisce negando le

accuse e affermando di essere vittima di un attacco. Di attacco coordinato, diffamazione, macchina del fango parla anche una lettera pubblica a suo sostegno firmata da alcuni ricercatori, giornalisti e attivisti, molti di area Wikileaks. Il punto principale del contendere è il fatto che le accuse di molestie sessuali (così le aveva formulate Tor, ma il sito e il profilo anonimi, oltre che alcune sviluppatrici del progetto, avevano menzionato anche la parola "stupro" o "stupratore") non sarebbero abbastanza circostanziate o evidenti, né sarebbero state mostrate delle prove. Non è chiaro se queste prove manchino o se Tor non intenda esporle per proteggere le vittime. Quello che è chiaro – mentre veleni, accuse pesanti e personali cominciano a rimbalzare da una parte all'altra degli schieramenti, cioè tra sostenitori e detrattori di Appelbaum, in una sorta di contagio collettivo e di avvelenamento progressivo della scena attivista – è che non esisterebbe alcuna indagine penale a suo carico (almeno mentre sto scrivendo). E che la dirigenza di Tor appare molto ferma e determinata nelle sue posizioni.

A luglio il progetto torna infatti con un ulteriore comunicato in cui annuncia una indagine interna sulle presunte accuse di molestie, affermando di aver avuto conferma di molteplici episodi sia dentro che fuori l'organizzazione. "Alcuni di questi incidenti sono stati condivisi pubblicamente; altri no", scrive Shari Steele, che annuncia anche una nuova policy per affrontare simili casi all'interno dell'organizzazione.

"Stabilire delle procedure è più difficile per il progetto Tor rispetto ad altre associazioni, perché il nostro staff lavora a stretto contatto con una più ampia comunità, fatta in gran parte di volontari o impiegati di altre organizzazioni. Non si tratta di un ambiente tradizionale e verticale", precisa ancora Steele. La quale si adopera anche per rinnovare il consiglio direttivo del progetto: fra i nuovi ingressi, diverse figure di spicco del mondo accademico, attivista o della sicurezza informatica, come l'antropologa Gabriella Coleman, il noto crittografo Bruce Schneier, il ricercatore Matt Blaze. Un parterre autorevole che sembra essere stato scelto apposta per fortificare il progetto in vista di attacchi futuri.

Intanto, però, a indebolirlo sono i suoi dissidi interni. Mentre la testata tedesca "Zeit" ritorna sul caso Appelbaum con una inchiesta che sembra smontare alcune delle accuse mosse contro di lui, e firmata da un nome importante nel settore, Christian Fuchs, un accademico specializzato su

Internet e sorveglianza, un gruppo non ben identificato lancia in Rete l'idea di uno sciopero di Tor: una giornata in cui gli operatori dei suoi nodi avrebbero dovuto staccare la spina per protestare contro il trattamento riservato ad Appelbaum e chiedere le dimissioni di Steele e Dingledine. L'idea – lanciata con una lettera anonima online – verrà bollata come controversa, se non addirittura stupida, da molti membri della comunità e non avrà un vero traino. Mostra però il grado di tensione raggiunto. E determina l'allontanamento di altri volontari dal progetto.

Ma non si tratta solo di questo. Fra le contestazioni mosse a Tor da chi chiede lo sciopero, ci sarebbero anche relazioni troppo disinvolte tenute dal gruppo dirigente con la comunità dell'intelligence americana. Emerge infatti che era stato assunto, in verità per un breve periodo, e all'insaputa di molti dipendenti di Tor, un uomo che in passato aveva lavorato per la Cia. Poi ci sono legami personali di alcuni suoi membri. Del resto, lo stesso Dingledine un tempo aveva fatto una sorta di stage alla Nsa. Ma anche questo è un terreno scivoloso: data l'origine di Tor e il particolare humus americano, dove convivono gomito a gomito tecnologia, ricerca statale, aziende della Silicon Valley, ricercatori e attivisti, che esistano delle relazioni e dei punti di contatto non stupisce molto. Altro discorso è se essi diventano un presidio per condizionare il progetto.

Parlando con vari membri della comunità di Tor, la preoccupazione principale è molto più pratica: è la dipendenza economica dal governo americano. Che però finora sembra più voler aiutare lo sviluppo del progetto che sabotarlo. Nel 2014 la Darpa è tornata a finanziare Tor e in particolare una serie di programmi legati ai suoi "servizi nascosti"[33], vale a dire al Dark Web. Una mossa non da poco, in quanto questa componente di Tor, per quanto minoritaria per traffico, è quella che attira più critiche dai suoi detrattori, dal momento che consente la realizzazione e la gestione nell'anonimato di siti illegali.

Tra questi programmi di finanziamento, oltre allo sviluppo di un motore di ricerca chiamato Memex, c'è addirittura l'obiettivo di rafforzare i "servizi nascosti" nei confronti di cyber-attacchi diretti contro di loro. L'obiettivo di tali progetti, incluso il motore di ricerca Memex, "non è denanonimizzare qualsiasi utente Tor", è scritto sul sito della Darpa, né di "accedere a informazioni che non vogliono essere pubbliche". Anzi. In pratica Darpa e Tor stanno lavorando a una nuova generazione di darknet,

fortificando perfino la sua crittografia e introducendo nuove funzioni come la possibilità di gestire un servizio nascosto da multipli host in modo da reagire meglio a cyber-attacchi che puntino a sommergere un sito di richieste. Tutto ciò mentre sui media tradizionali il Dark Web continua ad essere additato solo come rifugio per traffici inenarrabili. Ma, come abbiamo visto, la sua storia, e probabilmente anche il suo futuro, sono molto più sfumati e complessi.

[30] Tra gli altri, l'ormai abbandonato Free Haven, un sistema per conservare dati in modo anonimo, decentralizzato e resistente a forme di censura.

[31] Col termine "relay" il progetto Tor indica i nodi o router della sua rete che smistano il traffico. I nodi Tor sono gestiti da volontari, individui o associazioni.

[32] Il whistleblowing (letteralmente, in inglese: "soffiare nel fischietto") indica la denuncia di fenomeni di corruzione o abuso in una organizzazione da parte di suoi dipendenti. Il whistleblower dunque è più che un informatore o una talpa, termini che in italiano non hanno accezione positiva. Nel 2016 l'Accademia della Crusca ha proposto di tradurlo con "allertatore civico". Scrive la Crusca: "L'angloamericanismo, presente nella stampa italiana con qualche rara occorrenza fin dagli anni Novanta, si è ampiamente diffuso nel 2013 in relazione al 'caso Snowden'. L'allertatore civico è colui che, dopo aver constatato sistematiche irregolarità all'interno dell'organizzazione pubblica o privata per cui lavora, decide di denunciare l'illecito per il bene della collettività".

[33] Con "servizi nascosti" ("hidden services"), nel progetto Tor si intende la possibilità di realizzare servizi Internet (siti web, chat, ecc.) il cui indirizzo Ip resti nascosto agli utenti. Insomma, siti e servizi anonimi e non localizzabili, così come lo sono gli utenti che lo usano per navigare.

9.
Vi presento: gli “attivisti della Rete”

A Valencia, nel nome della libertà digitale

È forse l’unico evento sulla Rete in cui ai partecipanti si chiede di non twittare. O, quanto meno, di non pubblicare i nomi dei partecipanti senza il loro consenso. Per non dire delle fotografie, del tutto proibite. Te lo ricordano gli organizzatori quando ti iscrivi all’ingresso, lo ribadiscono i cartelli. Perché se questo è il festival per un Internet libero, chi vi prende parte arriva da Paesi che non lo sono. E ci sono degli accorgimenti di sicurezza da rispettare.

Così, entrando nelle aule e nei cortili dell’Internet Freedom Festival – raduno globale di comunità e gruppi digitali provenienti da 40 Paesi diversi, 78 città, per oltre 600 partecipanti, che si è tenuto nel marzo 2016 a Valencia, in Spagna, all’interno di Las Naves, spazio di collaborazione creativa fatto di classi, aule computer, biblioteche, sale, cortili, divanetti, bar – si materializzano di colpo i famosi “attivisti della Rete”, che spesso, quando vengono evocati, sembrano quasi delle astratte idee platoniche; e qua invece te li trovi davanti tutti assieme, immersi in progetti concreti.

Messico, Nigeria, Libano, Egitto, Iran, Cuba, Vietnam sono alcuni dei Paesi da cui sono arrivati i partecipanti, oltre che Spagna, Germania, Stati Uniti, Italia. I temi sul piatto? Il binomio sorveglianza e censura, certo, ma anche l’inclusione sociale attraverso la Rete, l’uso del digitale per rinnovare la democrazia dal basso, la lotta alle molestie e alle discriminazioni online. E molto altro. È qui che incontro Femi, un giovane di Lagos, che fa parte di un laboratorio sociale, Co-Creation Hub, per trovare soluzioni creative e tech ad alcuni dei problemi della Nigeria. E che, tra le altre cose, mi

racconta di come nel 2015 abbia dovuto difendere uno dei giornali d'opposizione, "Premium Times", da una serie di attacchi informatici che cercavano di mandarlo offline durante le elezioni. "Lavoriamo molto sulla sicurezza digitale delle organizzazioni", mi dice tra un seminario e l'altro, nel cortile dove due furgoncini colorati sfornano panini e birra a tutte le ore: da una parte carne, dall'altra piatti vegan.

La gente sciama chiacchierando tra le aule e le sale computer in maglietta, infradito e zainetti. Tanti i laptop aperti sulle ginocchia, pochi quelli che stanno chini su uno smartphone. E sui biglietti da visita non manca mai l'impronta digitale della chiave Pgp per scriversi mail cifrate.

In effetti, la difesa digitale di persone e gruppi è uno dei grandi temi del festival. E non solo per chi viene dal Sud del mondo. Come ad esempio Matt Mitchell. È stato sviluppatore alla Cnn e data journalist al "New York Times". Ora organizza "cripto-party" ad Harlem, New York. Si tratta di eventi in cui si insegna a nascondere le proprie tracce online e a difendere le proprie comunicazioni digitali da avversari che potrebbero volerle usare in modo malevolo, anche solo per scopi di profilazione. In particolare, Mitchell lavora con le comunità marginalizzate, o politicizzate, o più nel mirino della sorveglianza statale, anche quando non commettono alcun reato: come gli attivisti afroamericani del movimento Black Lives Matter, gli animalisti e via dicendo.

"Il problema principale è avere la loro fiducia", mi dice Mitchell, che incontro in un seminario su come parlare di questi temi all'uomo della strada. E dove le domande sollevate dai partecipanti disposti a cerchio nella stanza sono più delle risposte. Come trovare prove di sorveglianza mirata su specifici attivisti? Come attribuirle a qualcuno? E come evitare che l'uso della crittografia non renda sospetto, se non addirittura illegale, quello che fai agli occhi delle autorità? E cosa replicare a chi dice: "tanto siamo tutti sorvegliati e comunque non ho nulla da nascondere?".

Le stesse domande che Viktor, un giovane nerd di Berlino, mi pone alla fine del seminario, in una pausa al bar. "Come si fa a parlarne alla maggioranza della popolazione?", mi chiede con più entusiasmo che sconforto. Lui proviene dalla capitale degli attivisti digitali, da dove non a caso sono giunti in molti, inclusi gli storici hacker del Chaos Computer Club. Il giorno dopo, Viktor condurrà un altro seminario proprio sulle conseguenze della sorveglianza: si parte con autocensura, isolamento,

paranoia, e si scala, a seconda degli Stati e delle situazioni, a vere e proprie molestie, attacchi mirati, in casi estremi incarcerazione e morte. Purtroppo, gli esempi reali, in molte parti del mondo, non mancano.

Con Micah Lee, invece, si va molto più sul pratico. Lui è un noto sviluppatore che è stato assunto dalla testata americana "The Intercept", quella fondata dal giornalista Glenn Greenwald, uno dei reporter che ha preso contatto con Edward Snowden e ha lavorato sui documenti del Datagate. Compiti di Lee sono la messa in sicurezza del sito, ma anche delle comunicazioni dei suoi giornalisti, e la gestione di documenti delicati (a partire da quelli di Snowden). Al festival di Valencia sta tenendo degli incontri su questi temi. "Abbiamo diversi livelli di protezione a seconda dei documenti a 'The Intercept'. Alcuni di questi restano completamente sconnessi dalla Rete ovviamente", mi dice.

In quanto alle raccomandazioni per i giornalisti, Lee ricorda l'importanza di incoraggiare le proprie fonti a usare canali sicuri, già a partire dal primo contatto se possibile. Ed è proprio questa, da quanto emerge anche dagli altri workshop sul tema, la sfida più difficile: il primo contatto. Non bisogna dimenticare che ci sono Paesi in cui chi denuncia abusi e corruzione rischia moltissimo, anche la vita. Lo sanno bene Carlos e Vladimir di R3D, la rete di difesa dei diritti digitali in Messico, che opera in un contesto permeato da violenza, uccisioni e sparizioni. Un movimento che mescola attivismo offline e online, e che si è dotato anche di un sito per soffiate anonime, MexicoLeaks, basato su una piattaforma sviluppata da italiani, GlobaLeaks.

L'anonimato per proteggere le fonti che vogliano mandare segnalazioni senza esporsi è garantito dalle darknet, ovvero dal tanto deprecato Dark Web. Non è una novità: da anni testate autorevoli come "Forbes" o "The New Yorker" (e in Italia, più recentemente, "l'Espresso" con RegeniLeaks) hanno creato siti nelle darknet per aiutare potenziali fonti a farsi avanti in modo anonimo. E ci sono anche autorità nazionali che hanno abbracciato queste tecnologie per favorire la denuncia di casi di corruzione.

Su siti anticorruzione lavorano anche gli attivisti spagnoli di Xnet, che hanno anticipato molti temi di democrazia digitale successivamente ripresi (copiati, dicono loro) dal movimento Podemos. "Stiamo anche cercando di mettere in piedi dei servizi online alternativi a quelli offerti dalle grandi

aziende, tipo Dropbox, ecc.”, mi racconta Maddish Falzoni, una energica sistemista di Xnet che ha vissuto anche in Italia.

I software per l’anonimato, e chi ci lavora, sono una componente centrale di queste comunità. Tanto è vero che qui a Valencia, perlopiù radunati in biblioteca e mimetizzati dietro a laptop cosparsi di adesivi pro-privacy, si trovano gran parte degli sviluppatori del progetto Tor, il software più diffuso per proteggere la propria identità online e su cui è edificata buona parte del cosiddetto Dark Web, come abbiamo appena visto. Mescolati, in piccoli gruppi, con membri della Aclu, la storica associazione americana per le libertà civili. O della battagliera Electronic Frontier Foundation, testa di ponte delle lotte digitali. O di Amnesty International. Proprio Amnesty, mi racconta Milena Marin – d’origine rumena, italiano perfetto, residente a Londra dove lavora al segretariato internazionale della Ong –, sta pensando ad alcuni progetti per superare l’attivismo da “clicca la petizione”. Uno di questi prevede di coinvolgere le persone per riuscire a individuare su mappe satellitari, divise in frammenti, eventuali segni di danni ambientali. Sono partiti con le immagini di un canale in Nicaragua.

Insomma, all’Internet Freedom Festival di Valencia si respira e si tocca con mano la realtà dell’attivismo digitale, che è tutto fuorché una mobilitazione da mouse e clic facili. E in cui non sembrano esserci barriere tra Nord e Sud del mondo, fra democrazie e Stati autoritari: i partecipanti, pur vivendo in contesti nettamente differenti, con ben diversi diritti, garanzie e rischi, parlano comunque una stessa lingua.

La resistenza ai censori cinesi

Sarà in un raduno di questo tipo, ma che non posso menzionare per questioni di sicurezza, che incontrerò di persona Charlie Smith. Si tratta di uno pseudonimo, naturalmente, perché la sua vera identità deve restare segreta. Smith è infatti uno dei tre anonimi attivisti dietro a GreatFire, una organizzazione che combatte contro il cosiddetto Great Firewall, ovvero il complesso sistema tecnologico messo in piedi dalla Cina per censurare Internet.

“GreatFire è nato cinque anni fa, con l’idea di informare i cinesi su come funzionavano i meccanismi della censura”, mi dice Smith, dopo essersi assicurato della mia identità. Lui e gli altri due fondatori del progetto sono

anonimi e non si sono mai incontrati. Inoltre, anche nel posto dove ci siamo visti, l'uomo deve mantenere un basso profilo. "Ci sono due aspetti della censura cinese: il primo ha a che fare con il blocco di siti stranieri, come Facebook, Wikipedia, organizzazioni per i diritti umani, alcuni media; il secondo, più serio, riguarda invece la censura interna di contenuti su siti cinesi, come Weibo [una sorta di Twitter locale], che sta morendo per quanto è ormai censurato. C'è una minoranza di persone che usano strumenti per aggirare la censura, ma le autorità stanno dando un giro di vite su questi mezzi, come le Vpn [o Tor, che pur essendo a sua volta bloccato sfrutta dei metodi alternativi, dei nodi 'nascosti', chiamati 'bridge', per essere accessibile dalla Cina]".

Smith e i suoi compagni di avventura si sono inventati un metodo, quello della Collateral Freedom (libertà collaterale)[34]. L'idea è che anche per i censori cinesi ci siano delle risorse troppo preziose per essere censurate. Ad esempio un sito come GitHub, usato da sviluppatori di tutto il mondo per pubblicare i loro progetti. E soprattutto un servizio che usa connessioni cifrate. "Se un sito implementa la cifratura, i censori devono decidere se bloccarlo tutto o per nulla". Non possono cioè filtrare solo una sua singola pagina. Così GitHub ospita i contenuti di GreatFire. Come FreeWeibo, un sito dove sono ripubblicati i messaggi censurati sui social cinesi. O Free Browser, una app per Android che naviga attraverso server esterni alla Cina, permettendo di circumnavigare la censura. O l'elenco dei siti e delle parole chiave bloccate dal governo centrale.

Per questo nel 2015 la Cina ha provato a bombardare la pagina di GreatFire su GitHub con un potente e sofisticato attacco informatico di tipo DDoS (che consiste nel sovraccaricare di traffico un sito o un server). Il sistema usato – ribattezzato Great Cannon, "grande cannone" – era particolarmente insidioso perché attraverso una società di telecomunicazioni e Isp cinese, China Unicom, si inseriva nel traffico Internet di visitatori di siti web che usavano gli "analytics" – cioè i servizi di analisi delle statistiche e di tracciamento degli utenti – del motore di ricerca cinese Baidu, e poi iniettava nei loro browser un codice malevolo che si metteva a caricare la pagina GitHub che ospitava GreatFire. Il risultato era un eccesso di traffico che mandava offline quei contenuti. In pratica si sequestrava il traffico di utenti innocenti per usarlo come un'arma a loro insaputa, trasformandoli nei soldatini di un attacco distribuito di

negazione del servizio (DDoS). Tuttavia, alla fine i contenuti sono ancora lì. "Sono dei campioni della libertà", dice Smith riferendosi a GitHub.

Il ruolo delle aziende

Attacchi informatici, disinformazione, censura, sorveglianza. Lo scenario dei futuri conflitti di Rete mescolerà tutti questi elementi, spesso camuffandoli per qualcosa che non sono. Per questo vorrei concludere questo libro parlando del lavoro di una giovane donna. Si chiama Maria Xynou, ha origini greche e sudafricane, ha vissuto in vari Paesi e quando la intervisto – al tavolino di un bar al Festival del Giornalismo di Perugia – vive e lavora a Berlino, nell'organizzazione Tactical Tech, che produce strumenti e workshop di consapevolezza e autodifesa digitale.

Maria è l'emblema di una generazione nuova, estremamente cosmopolita, tecnologicamente esperta, politicizzata, precoce, precisa, pratica. È l'opposto dell'immagine mediatica dei bamboccioni, o dei nerd chiusi in mondi virtuali, o di indignati ideologici fini a se stessi. "Quando ero a scuola non capivo davvero come i miei compagni potessero stare su MySpace, come potessero mettere in mostra le proprie informazioni", mi dice ridendo. Aveva perfino avviato una petizione contro uno dei primi reality in tv, una trasmissione dove veniva massacrato qualsiasi concetto di privacy. "Ma nessuno la firmò", mi dice Maria. "Allora ragionai: o sono pazza io, o il problema è più grave di quanto si pensi".

Da allora ha cercato di studiare e capire i meccanismi di sorveglianza e autosorveglianza, e come questi si intreccino tra bisogni individuali, spinte di mercato e poteri statali. "I social media hanno amplificato la questione, perché si basano su un illusorio senso di libertà che ti rende ancora più facile da sorvegliare, attraverso il meccanismo della condivisione spontanea. Forse stiamo vivendo all'interno di un nuovo sistema politico, una sorta di infocrazia. Ma allora bisogna chiedersi: chi controlla oggi l'informazione? E quale ruolo giocano le corporation in questo sistema?". Così, insieme allo sviluppatore italiano Claudio Agosti e ad altri, Maria ha lavorato a Trackography, un progetto di monitoraggio dedicato solo alle aziende: è una mappa interattiva che analizza come i lettori dei principali siti di informazione (hanno scelto apposta i media a titolo esemplificativo, ma il discorso vale per quasi tutti i siti) siano tracciati nei loro

comportamenti e spostamenti online da una miriade di altre aziende, che condividono e si rivendono i loro dati.

L'altro progetto su cui ha lavorato è invece più legato al tema "classico" del controllo statale. Ma anche in questo caso, l'attenzione è alle sinergie Stati-imprese. "Quando sono usciti i documenti di Edward Snowden sul Datagate ero frustrata dalla difficoltà di trovare informazioni specifiche. Quali documenti contenevano indicazioni utili per gli attivisti? O erano relative a uno Stato in particolare? O a un'azienda? Avevo l'impressione che stessimo seduti su una miniera di informazioni non adeguatamente sfruttate", mi dice.

Allora è andata a prendersi tutti i documenti usciti su quel tema e manualmente, uno dopo l'altro, ne ha estratto una serie di informazioni suddividendole in categorie e costruendo una mappa. Ora si possono cercare questi documenti per Paese o per tema. Si vogliono analizzare informazioni sui programmi di sorveglianza mirata o di massa? O sul ruolo dei privati o sulle collaborazioni fra intelligence? Surveillance Without Borders (sorveglianza senza frontiere, questo il nome del sito[35] e del progetto di Maria, realizzato insieme allo sviluppatore italiano Arturo Filastò) fa proprio questo. Uno strumento costato innumerevoli serate di lavoro volontario, ora a disposizione di giornalisti, ricercatori, attivisti.

Così facendo, anche questa volta, così come le era capitato in passato mentre si trovava in India, o quando era una stagista nella Ong Privacy International, la sua attenzione è stata attirata dal ruolo delle aziende. "Voglio concentrarmi sulla sorveglianza corporate perché trovo interessante il suo ruolo nell'ecosistema globale: a volte le imprese erano vittime della sorveglianza statale; a volte erano alleate; a volte entrambe le cose; e, a volte, non era chiaro".

I futuri conflitti di Rete saranno così, almeno ancora per un po' di tempo: grandi e piccole industrie, Stati, gruppi parastatali o criminali si rimescoleranno o scontreranno o affiancheranno in un risiko di interessi estremamente tattico e mutevole. E in uno scenario difficile da decifrare.

L'unico dato certo, finora, è che a farne le spese saranno sempre di più i normali cittadini, gli utenti da cannone. E che con loro potrebbero pagare dazio lo Stato di diritto, la privacy come bene strettamente connesso alla libertà e alla democrazia, e chi si espone più di altri per la loro difesa. Quella che stiamo vivendo è ancora una finestra di opportunità. Che però

è destinata a chiudersi ogni giorno di più se non incontrerà una resistenza consapevole da parte di una massa critica di persone.

[34] https://www.teamupturn.com/static/files/CollateralFreedom.pdf.
[35] https://surveillancewithoutborders.com.

Bibliografia

AA.VV., *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s*, in “New America”, 17 giugno 2015.

AA.VV., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, in “Dspace@MIT”, 6 luglio 2015.

AA.VV., *Know Your Enemies 2.0: The Encyclopedia of the Most Prominent Hacktivists, Nation State and Mercenaries Hackers*, Institute for Critical Infrastructure Technology, 8 febbraio 2016.

AA.VV., *The ICIT Ransomware Report*, Institute for Critical Infrastructure Technology, 7 marzo 2016.

AA.VV., *Your Life, Repackaged and Resold: The Deep Web Exploitation of Health Sector Breach Victims*, Institute for Critical Infrastructure Technology, 6 settembre 2016.

Julian Assange, *Internet è il nemico. Conversazione con Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann*, Feltrinelli, Milano 2013.

Abdel-Bari Atwan, *Islamic State: The Digital Caliphate*, Saqi Books, London 2015.

Carola Frediani, *Deep Web. La Rete oltre Google*, Stampa Alternativa, Roma 2016 (riedizione aggiornata dell’ebook edito da Quintadicopertina, 2014).

Carola Frediani, Stefano Rizzato, Bruno Ruffilli, Massimo Russo, Raphaël Zanotti, *Attacco ai pirati. L’affondamento di Hacking Team: tutti i segreti del datagate italiano*, La Stampa, Torino 2015.

Eric Geller, *A Complete Guide to the New ‘Crypto Wars’*, in “Daily Dot”, 26 aprile 2016.

Glenn Greenwald, *Sotto controllo. Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano 2014.

Shane Harris, *@War: The Rise of the Military-Internet Complex*, Mariner Books, Boston 2015.

Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*, Sourcebooks, Chicago 2015.

Kaspersky Lab, *KSN Report: Ransomware in 2014-2016*, in “Securelist.com”, 22 giugno 2016.

Kevin Poulsen, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*, Broadway Books, Portland 2012.

Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton, New York 2016.

Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, PublicAffairs, New York 2016.

Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, New York 2014.
Giovanni Ziccardi, *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina, Milano 2016.

Glossario

Apt: “Advanced persistent threat”, ovvero “minaccia persistente avanzata”, indica un soggetto collettivo che compie attacchi informatici mirati, prolungati nel tempo e sofisticati contro target di un certo livello. In genere si tratta di un gruppo cyber-criminale o parastatale, o di una emanazione di un’agenzia nazionale. Tra i suoi obiettivi: cyber-spionaggio, sabotaggio, furto di dati finanziari e di asset.

Backdoor: è la “porta di servizio”, ovvero un sistema che consente di accedere a un dispositivo (o a un software) aggirando i suoi sistemi di identificazione e protezione.

Bitcoin: è la più nota moneta elettronica basata sulla crittografia e su una rete distribuita di tipo “peer-to-peer”, cioè una rete in cui non ci sono differenze gerarchiche fra i suoi nodi (un esempio noto di rete peer-to-peer è quella usata nel file sharing). Tra le sue caratteristiche, la possibilità di garantire un buon livello di anonimato a chi la usa, se si adottano alcuni stratagemmi. C’è chi preferisce la definizione di “moneta matematica” proprio per sottolineare l’uso della crittografia per creare valuta e rendere sicure le transazioni (di qui i termini “cripto-valuta”, “cripto-moneta”, ecc.).

Crittografia: (da *kryptós*, “nascosto”, e *graphía*, “scrittura”) è lo studio dei metodi per offuscare le informazioni. Nella sua accezione più moderna, e nel contesto di questo libro, indica la disciplina e le tecniche impiegate per proteggere l’integrità e la segretezza di alcune informazioni digitali convertendole in forma cifrata (e quindi illeggibile). Solo l’uso di una chiave segreta può convertire (decifrare) i messaggi in una forma di nuovo leggibile.

Darknet: sono le reti create attraverso software appositi, come Tor, dove possono restare anonimi sia coloro che gestiscono un sito web o un servizio, sia i loro utenti. L’insieme di siti e servizi nascosti in queste reti, non raggiungibili dai motori di ricerca o dai browser più comuni, è spesso definito, giornalisticamente, Dark Web o Deep Web.

Exploit: è un codice informatico scritto per sfruttare una vulnerabilità – un errore o un difetto di un software o di un sistema – attraverso la quale si può realizzare un attacco.

Malware: da “malicious software”, ovvero “software malevolo”, progettato per danneggiare o infiltrare un altro software. Un termine ombrello che raccoglie software malevoli dalle diverse specificità: virus, worm, trojan, ransomware, spyware, adware, ecc.

Ransomware: da "ransom", cioè "riscatto", e "software", indica software malevoli che limitano l'accesso degli utenti a un sistema finché questi non pagano un riscatto. Nella loro forma più moderna, i crypto-ransomware, cifrano i file del pc. E per decifrarli occorre recuperare la chiave.

Spyware: è un software malevolo che, una volta installato, spia alcune o quasi tutte le attività dell'utente, per sottrarre dati e monitorare comunicazioni. Spesso, per indicare questo software, viene utilizzato anche il termine "trojan" (da "trojan horse", "cavallo di Troia"), che tecnicamente indicherebbe un malware usato per hackerare un computer, in genere mimetizzandolo come qualcosa di diverso (un altro programma o un documento). Di qui il riferimento al cavallo di Troia.

Tor: è un software libero che permette di navigare e comunicare in modo anonimo in Internet. Può essere inoltre utilizzato per realizzare siti e servizi Internet a loro volta anonimi. Su software come Tor si fondano dunque gran parte delle darknet.

Vpn: "Virtual private network", cioè "rete privata virtuale", è una tecnologia che stabilisce una connessione cifrata sopra un'altra rete meno sicura (come Internet). È usata dalle aziende per accedere dall'esterno al proprio network, ma le Vpn possono essere anche uno strumento per navigare mascherando la propria identità (il proprio indirizzo Ip) e per aggirare filtri e censure. Se vivo in Turchia e non posso accedere a YouTube perché il governo ha censurato quel sito, collegandomi prima a una Vpn che ha i server in Svezia potrò navigare come se mi trovassi lì (e quindi connettermi anche a YouTube).

Vulnerabilità: nel mondo della sicurezza informatica si intende una falla nella sicurezza di un prodotto che lo sviluppatore non intendeva introdurre e che dovrebbe essere aggiustata una volta scoperta.

Zero-day: è un exploit ancora sconosciuto agli sviluppatori di un software, per cui questi non hanno avuto a disposizione alcun giorno (zero, appunto) per chiudere la falla sfruttata da quel codice di attacco.

Ringraziamenti

Vorrei ringraziare ovviamente tutte le persone intervistate in questo libro, che hanno accettato di rispondere alle mie domande indipendentemente da quello che fanno.

Poi, un grazie speciale a Paolo Dal Checco, le cui conoscenze di informatica forense sono equiparabili forse solo alla sua disponibilità e chiarezza espositiva; a Mattia Epifani e al suo collega Francesco Picasso, che mi hanno accolto più volte nel loro studio aiutandomi a capire questioni abbastanza complesse; ad Alberto Pelliccione, una delle menti più brillanti del mondo "infosec" ("infosecurity") e dalle infinite conoscenze al riguardo, oltre che campione di pazienza nel rispondere alle domande più improbabili; e, *last but not least*, ad Andrea Raimondi, che da duemila chilometri di distanza non solo mi ha incoraggiata e sostenuta, ma ha anche letto e annotato la prima stesura con una competenza e un entusiasmo davvero rari.